3-7-00

A

Practitioner's Docket No. 324-009249-US(PAR) **PATENT**

Preliminary Classification:

Proposed Class:

Subclass:

NOTE: "All applicants are requested to include a preliminary classification on newly filed patent applications. The preliminary classification, preferably class and subclass designations, should be identified in the upper right-hand corner of the letter of transmittal accompanying the application papers, for example 'Proposed Class 2, subclass 129.'" M.P.E.P. § 601, 7th ed.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

NEW APPLICATION TRANSMITTAL

Transmitted herewith for filing is the patent application of

Inventor(s): Jukka VIALEN, Fabio LONGONI

WARNING: *37 C.F.R. § 1.41(a)(1) points out:*

"(a) A patent is applied for in the name or names of the actual inventor or inventors.

"(1) The inventorship of a nonprovisional application is that inventorship set forth in the oath or declaration as prescribed by § 1.63, except as provided for in § 1.53(d)(4) and § 1.63(d). If an oath or declaration as prescribed by § 1.63 is not filed during the pendency of a nonprovisional application, the inventorship is that inventorship set forth in the application papers filed pursuant to § 1.53(b), unless a petition under this paragraph accompanied by the fee set forth in § 1.17(i) is filed supplying or changing the name or names of the inventor or inventors."

For (title): METHOD OF CIPHERING DATA TRANSMISSION IN A RADIO SYSTEM

CERTIFICATION UNDER 37 C.F.R. § 1.10*
(Express Mail label number is mandatory.)
(Express Mail certification is optional.)

I hereby certify that this New Application Transmittal and the documents referred to as attached therein are being deposited with the United States Postal Service on this date March 6, 2000, in an envelope as "Express Mail Post Office to Addressee," mailing Label Number EL336863425US, addressed to the: Assistant Commissioner for Patents, Washington, D.C. 20231.

Deborah J. Clark

(type or print name of person mailing paper)

Deborah J. Clark

Signature of person mailing paper

WARNING: *Certificate of mailing (first class) or facsimile transmission procedures of 37 C.F.R. § 1.8 cannot be used to obtain a date of mailing or transmission for this correspondence.*

***WARNING:** Each paper or fee filed by "Express Mail" **must** have the number of the "Express Mail" mailing label placed thereon prior to mailing. 37 C.F.R. § 1.10(b).*
*"Since the filing of correspondence under § 1.10 without the Express Mail mailing label thereon is an oversight that can be avoided by the exercise of reasonable care, requests for waiver of this requirement will **not** be granted on petition." Notice of Oct. 24, 1996, 60 Fed. Reg. 56,439, at 56,442.*

1. Type of Application

This new application is for a(n)

(check one applicable item below)

☒ Original (nonprovisional)

☐ Design

☐ Plant

WARNING: ***Do not*** *use this transmittal for a completion in the U.S. of an International Application under 35 U.S.C. § 371(c)(4), unless the International Application is being filed as a divisional, continuation or continuation-in-part application.*

WARNING: ***Do not*** *use this transmittal for the filing of a provisional application.*

NOTE: If one of the following 3 items apply, then complete and attach ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF A PRIOR U.S. APPLICATION CLAIMED and a NOTIFICATION IN PARENT APPLICATION OF THE FILING OF THIS CONTINUATION APPLICATION.

☐ Divisional.

☐ Continuation.

☐ Continuation-in-part (C-I-P).

2. Benefit of Prior U.S. Application(s) (35 U.S.C. §§ 119(e), 120, or 121)

NOTE: A nonprovisional application may claim an invention disclosed in one or more prior filed copending nonprovisional applications or copending international applications designating the United States of America. In order for a nonprovisional application to claim the benefit of a prior filed copending nonprovisional application or copending international application designating the United States of America, each prior application must name as an inventor at least one inventor named in the later filed nonprovisional application and disclose the named inventor's invention claimed in at least one claim of the later filed nonprovisional application in the manner provided by the first paragraph of 35 U.S.C. § 112. Each prior application must also be:

(i) An international application entitled to a filing date in accordance with PCT Article 11 and designating the United States of America; or

(ii) Complete as set forth in § 1.51(b); or

(iii) Entitled to a filing date as set forth in § 1.53(b) or § 1.53(d) and include the basic filing fee set forth in § 1.16; or

(iv) Entitled to a filing date as set forth in § 1.53(b) and have paid therein the processing and retention fee set forth in § 1.21(l) within the time period set forth in § 1.53(f).

37 C.F.R. § 1.78(a)(1).

NOTE: If the new application being transmitted is a divisional, continuation or a continuation-in-part of a parent case, or where the parent case is an International Application which designated the U.S., or benefit of a prior provisional application is claimed, then check the following item and complete and attach ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED.

WARNING: *If an application claims the benefit of the filing date of an earlier filed application under 35 U.S.C. §§ 120, 121 or 365(c), the 20-year term of that application will be based upon the filing date of the earliest U.S. application that the application makes reference to under 35 U.S.C. §§ 120, 121 or 365(c). (35 U.S.C. § 154(a)(2) does not take into account, for the determination of the patent term, any application on which priority is claimed under 35 U.S.C. §§ 119, 365(a) or 365(b).) For a c-i-p application, applicant should review whether any claim in the patent that will issue is supported by an earlier application and, if not, the applicant should consider canceling the reference to the earlier filed application. The term of a patent is not based on a claim-by-claim approach. See Notice of April 14, 1995, 60 Fed. Reg. 20,195, at 20,205.*

WARNING: *When the last day of pendency of a provisional application falls on a Saturday, Sunday, or Federal holiday within the District of Columbia, any nonprovisional application claiming benefit of the provisional application* ***must*** *be filed prior to the Saturday, Sunday, or Federal holiday within the District of Columbia. See 37 C.F.R. § 1.78(a)(3).*

☐ The new application being transmitted claims the benefit of prior U.S. application(s). Enclosed are ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED.

3. Papers Enclosed

A. Required for filing date under 37 C.F.R. § 1.53(b) (Regular) or 37 C.F.R. § 1.153 (Design) Application

17 Pages of specification

6 Pages of claims

13 Sheets of drawing

WARNING: ***DO NOT*** *submit original drawings. A high quality copy of the drawings should be supplied when filing a patent application. The drawings that are submitted to the Office must be on strong, white, smooth, and non-shiny paper and meet the standards according to § 1.84. If corrections to the drawings are necessary, they should be made to the original drawing and a high-quality copy of the corrected original drawing then submitted to the Office. Only one copy is required or desired. For comments on proposed then-new 37 C.F.R. § 1.84, see Notice of March 9, 1988 (1990 O.G. 57-62).*

NOTE: "Identifying indicia, if provided, should include the application number or the title of the invention, inventor's name, docket number (if any), and the name and telephone number of a person to call if the Office is unable to match the drawings to the proper application. This information should be placed on the back of each sheet of drawing a minimum distance of 1.5 cm. (5/8 inch) down from the top of the page . . ." 37 C.F.R. § 1.84(c)).

(complete the following, if applicable)

☐ The enclosed drawing(s) are photograph(s), and there is also attached a "PETITION TO ACCEPT PHOTOGRAPH(S) AS DRAWING(S)." 37 C.F.R. § 1.84(b).

☐ formal

☐ informal

B. Other Papers Enclosed

7 Pages of declaration and power of attorney

1 Pages of abstract

_____ Other

4. Additional papers enclosed

☐ Amendment to claims

☐ Cancel in this applications claims _____ before calculating the filing fee. (At least one original independent claim must be retained for filing purposes.)

☐ Add the claims shown on the attached amendment. (Claims added have been numbered consecutively following the highest numbered original claims.)

☐ Preliminary Amendment

☐ Information Disclosure Statement (37 C.F.R. § 1.98)

☐ Form PTO–1449 (PTO/SB/08A and 08B)

☐ Citations

☐ Declaration of Biological Deposit

☐ Submission of "Sequence Listing," computer readable copy and/or amendment pertaining thereto for biotechnology invention containing nucleotide and/or amino acid sequence.

☐ Authorization of Attorney(s) to Accept and Follow Instructions from Representative

☐ Special Comments

☐ Other

5. Declaration or oath (including power of attorney)

NOTE: A newly executed declaration is not required in a continuation or divisional application provided that the prior nonprovisional application contained a declaration as required, the application being filed is by all or fewer than all the inventors named in the prior application, there is no new matter in the application being filed, and a copy of the executed declaration filed in the prior application (showing the signature or an indication thereon that it was signed) is submitted. The copy must be accompanied by a statement requesting deletion of the names of person(s) who are not inventors of the application being filed. If the declaration in the prior application was filed under § 1.47, then a copy of that declaration must be filed accompanied by a copy of the decision granting § 1.47 status or, if a nonsigning person under § 1.47 has subsequently joined in a prior application, then a copy of the subsequently executed declaration must be filed. See 37 C.F.R. §§ 1.63(d)(1)-(3).

NOTE: A declaration filed to complete an application must be executed, identify the specification to which it is directed, identify each inventor by full name including family name and at least one given name, without abbreviation together with any other given name or initial, and the residence, post office address and country or citizenship of each inventor, and state whether the inventor is a sole or joint inventor. 37 C.F.R. § 1.63(a)(1)-(4).

☒ Enclosed

Executed by

(check **all** *applicable boxes)*

☒ inventor(s).

☐ legal representative of inventor(s). 37 C.F.R. §§ 1.42 or 1.43.

☐ joint inventor or person showing a proprietary interest on behalf of inventor who refused to sign or cannot be reached.

☐ This is the petition required by 37 C.F.R. § 1.47 and the statement required by 37 C.F.R. § 1.47 is also attached. See item 13 below for fee.

☐ Not Enclosed.

NOTE: Where the filing is a completion in the U.S. of an International Application or where the completion of the U.S. application contains subject matter in addition to the International Application, the application may be treated as a continuation or continuation-in-part, as the case may be, utilizing ADDED PAGE FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION CLAIMED.

☐ Application is made by a person authorized under 37 C.F.R. § 1.41(c) on behalf of *all* the above named inventor(s).

(The declaration or oath, along with the surcharge required by 37 C.F.R. § 1.16(e) can be filed subsequently).

☐ Showing that the filing is authorized.
(not required unless called into question. 37 C.F.R. § 1.41(d))

6. Inventorship Statement

WARNING: *If the named inventors are each not the inventors of all the claims an explanation, including the ownership of the various claims at the time the last claimed invention was made, should be submitted.*

The inventorship for all the claims in this application are:

☐ The same.

or

☐ Not the same. An explanation, including the ownership of the various claims at the time the last claimed invention was made,

☐ is submitted.

☐ will be submitted.

7. Language

NOTE: An application including a signed oath or declaration may be filed in a language other than English. An English translation of the non-English language application and the processing fee of $130.00 required by 37 C.F.R. § 1.17(k) is required to be filed with the application, or within such time as may be set by the Office. 37 C.F.R. § 1.52(d).

☒ English

☐ Non-English

☐ The attached translation includes a statement that the translation is accurate. 37 C.F.R. § 1.52(d).

8. Assignment

☒ An assignment of the invention to Nokia Mobile Phones Ltd.

☒ is attached. A separate ☒ "COVER SHEET FOR ASSIGNMENT (DOCUMENT) ACCOMPANYING NEW PATENT APPLICATION" or ☐ FORM PTO 1595 is also attached.

☐ will follow.

NOTE: "If an assignment is submitted with a new application, send two separate letters-one for the application and one for the assignment." Notice of May 4, 1990 (1114 O.G. 77-78).

WARNING: *A newly executed "CERTIFICATE UNDER 37 C.F.R. § 3.73(b)" must be filed when a continuation-in-part application is filed by an assignee. Notice of April 30, 1993, 1150 O.G. 62-64.*

9. Certified Copy

Certified copy(ies) of application(s)

Country	Appln. No.	Filed
Finland	990500	8 March 1999
Country	Appln. No.	Filed
Country	Appln. No.	Filed

from which priority is claimed

☒ is (are) attached.

☐ will follow.

NOTE: The foreign application forming the basis for the claim for priority must be referred to in the oath or declaration. 37 C.F.R. § 1.55(a) and 1.63.

NOTE: This item is for any foreign priority for which the application being filed directly relates. If any parent U.S. application or International Application from which this application claims benefit under 35 U.S.C. § 120 is itself entitled to priority from a prior foreign application, then complete item 18 on the ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED.

10. Fee Calculation (37 C.F.R. § 1.16)

A. ☒ Regular application

CLAIMS AS FILED					
Number filed		Number Extra		Rate	Basic Fee 37 C.F.R. § 1.16(a) $ 690.00
Total Claims (37 C.F.R. § 1.16(c))	45 – 20 =	25	×	$ 18.00	450.00
Independent Claims (37 C.F.R. § 1.16(b))	3 – 3 =	0	×	$ 78.00	0
Multiple dependent claim(s), if any (37 C.F.R. § 1.16(d))			+	$260.00	

☐ Amendment cancelling extra claims is enclosed.

☐ Amendment deleting multiple-dependencies is enclosed.

☐ Fee for extra claims is not being paid at this time.

NOTE: If the fees for extra claims are not paid on filing they must be paid or the claims cancelled by amendment, prior to the expiration of the time period set for response by the Patent and Trademark Office in any notice of fee deficiency. 37 C.F.R. § 1.16(d).

Filing Fee Calculation $ 1,140.00

B. ☐ Design application
($310.00—37 C.F.R. § 1.16(f))

Filing Fee Calculation $_____

C. ☐ Plant application
($480.00—37 C.F.R. § 1.16(g))

Filing fee calculation $_____

11. Small Entity Statement(s)

☐ Statement(s) that this is a filing by a small entity under 37 C.F.R. § 1.9 and 1.27 is (are) attached.

WARNING: *"Status as a small entity must be specifically established in each application or patent in which the status is available and desired. Status as a small entity in one application or patent does not affect any other application or patent, including applications or patents which are directly or indirectly dependent upon the application or patent in which the status has been established. The refiling of an application under § 1.53 as a continuation, division, or continuation-in-part (including a continued prosecution application under § 1.53(d)), or the filing of a reissue application requires a new determination as to continued entitlement to small entity status for the continuing or reissue application. A nonprovisional application claiming benefit under 35 U.S.C. § 119(e), 120, 121, or 365(c) of a prior application, or a reissue application may rely on a statement filed in the prior application or in the patent if the nonprovisional application or the reissue application includes a reference to the statement in the prior application or in the patent or includes a copy of the statement in the prior application or in the patent and status as a small entity is still proper and desired. The payment of the small entity basic statutory filing fee will be treated as such a reference for purposes of this section." 37 C.F.R. § 1.28(a)(2).*

WARNING: *"Small entity status must not be established when the person or persons signing the . . . statement can **unequivocally** make the required self-certification." M.P.E.P., § 509.03, 6th ed., rev. 2, July 1996 (emphasis added).*

(complete the following, if applicable)

☐ Status as a small entity was claimed in prior application _____ / _____, filed on _____, from which benefit is being claimed for this application under:

35 U.S.C. § ☐ 119(e),
☐ 120,
☐ 121,
☐ 365(c),

and which status as a small entity is still proper and desired.

☐ A copy of the statement in the prior application is included.

Filing Fee Calculation (50% of **A, B** or **C** above)

$_____

NOTE: Any excess of the full fee paid will be refunded if small entitiy status is established and a refund request are filed within 2 months of the date of timely payment of a full fee. The two-month period is not extendable under § 1.136. 37 C.F.R. § 1.28(a).

12. Request for International-Type Search (37 C.F.R. § 1.104(d))

(complete, if applicable)

☐ Please prepare an international-type search report for this application at the time when national examination on the merits takes place.

13. Fee Payment Being Made at This Time

☐ Not Enclosed

☐ No filing fee is to be paid at this time.
(This and the surcharge required by 37 C.F.R. § 1.16(e) can be paid subsequently.)

☒ Enclosed

☒ Filing fee $ 1,140.00

☒ Recording assignment
($40.00; 37 C.F.R. § 1.21(h))
(See attached "COVER SHEET FOR ASSIGNMENT ACCOMPANYING NEW APPLICATION".) $ 40.00

☐ Petition fee for filing by other than all the inventors or person on behalf of the inventor where inventor refused to sign or cannot be reached
($130.00; 37 C.F.R. §§ 1.47 and 1.17(i)) $ _____

☐ For processing an application with a specification in a non-English language
($130.00; 37 C.F.R. §§ 1.52(d) and 1.17(k)) $ _____

☐ Processing and retention fee
($130.00; 37 C.F.R. §§ 1.53(d) and 1.21(l)) $ _____

☐ Fee for international-type search report
($40.00; 37 C.F.R. § 1.21(e)) $ _____

NOTE: 37 C.F.R. § 1.21(l) establishes a fee for processing and retaining any application that is abandoned for failing to complete the application pursuant to 37 C.F.R. § 1.53(f) and this, as well as the changes to 37 C.F.R. §§ 1.53 and 1.78(a)(1), indicate that in order to obtain the benefit of a prior U.S. application, either the basic filing fee must be paid, or the processing and retention fee of § 1.21(l) must be paid, within 1 year from notification under § 53(f).

Total fees enclosed $ 1,180.00

14. Method of Payment of Fees

☒ Check in the amount of $ 1,180.00

☐ Charge Account No. _____ in the amount of $_____.

A duplicate of this transmittal is attached.

NOTE: Fees should be itemized in such a manner that it is clear for which purpose the fees are paid. 37 C.F.R. § 1.22(b).

15. Authorization to Charge Additional Fees

WARNING: *If no fees are to be paid on filing, the following items should not be completed.*

WARNING: *Accurately count claims, especially multiple dependent claims, to avoid unexpected high charges, if extra claim charges are authorized.*

☒ The Commissioner is hereby authorized to charge the following additional fees by this paper and during the entire pendency of this application to Account No. 16-1350 :

☒ 37 C.F.R. § 1.16(a), (f) or (g) (filing fees)

☒ 37 C.F.R. § 1.16(b), (c) and (d) (presentation of extra claims)

NOTE: Because additional fees for excess or multiple dependent claims not paid on filing or on later presentation must only be paid or these claims cancelled by amendment prior to the expiration of the time period set for response by the PTO in any notice of fee deficiency (37 C.F.R. § 1.16(d)), it might be best not to authorize the PTO to charge additional claim fees, except possibly when dealing with amendments after final action.

☒ 37 C.F.R. § 1.16(e) (surcharge for filing the basic filing fee and/or declaration on a date later than the filing date of the application)

☒ 37 C.F.R. § 1.17(a)(1)–(5) (extension fees pursuant to § 1.136(a)).

☐ 37 C.F.R. § 1.17 (application processing fees)

NOTE: ". . .A written request may be submitted in an application that is an authorization to treat any concurrent or future reply, requiring a petition for an extension of time under this paragraph for its timely submission, as incorporating a petition for extension of time for the appropriate length of time. An authorization to charge all required fees, fees under § 1.17, or all required extension of time fees will be treated as a constructive petition for an extension of time in any concurrent or future reply requiring a petition for an extension of time under this paragraph for its timely submission. Submission of the fee set forth in § 1.17(a) will also be treated as a constructive petition for an extension of time in any concurrent reply requiring a petition for an extension of time under this paragraph for its timely submission." 37 C.F.R. § 1.136(a)(3).

☐ 37 C.F.R. § 1.18 (issue fee at or before mailing of Notice of Allowance, pursuant to 37 C.F.R. § 1.311(b))

NOTE: Where an authorization to charge the issue fee to a deposit account has been filed before the mailing of a Notice of Allowance, the issue fee will be automatically charged to the deposit account at the time of mailing the notice of allowance. 37 C.F.R. § 1.311(b).

NOTE: 37 C.F.R. § 1.28(b) requires "Notification of any change in status resulting in loss of entitlement to small entity status must be filed in the application . . . prior to paying, or at the time of paying, . . . the issue fee. . . " From the wording of 37 C.F.R. § 1.28(b), (a) notification of change of status must be made even if the fee is paid as "other than a small entity" and (b) no notification is required if the change is to another small entity.

16. Instructions as to Overpayment

NOTE: ". . . Amounts of twenty-five dollars or less will not be returned unless specifically requested within a reasonable time, nor will the payer be notified of such amounts; amounts over twenty-five dollars may be returned by check or, if requested, by credit to a deposit account." 37 C.F.R. § 1.26(a).

☒ Credit Account No. 16-1350

☐ Refund

SEND ALL CORRESPONDENCE TO:

SIGNATURE OF PRACTITIONER

Reg. No. 24,622

Clarence A. Green

(type or print name of attorney)

Tel. No. (203) 259-1800

PERMAN & GREEN, LLP

P.O. Address

Customer No.

425 Post Road, Fairfield, Connecticut 06430

☐ **Incorporation by reference of added pages**

(check the following item if the application in this transmittal claims the benefit of prior U.S. application(s) (including an international application entering the U.S. stage as a continuation, divisional or C-I-P application) and complete and attach the ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED)

☐ Plus Added Pages for New Application Transmittal Where Benefit of Prior U.S. Application(s) Claimed

Number of pages added _____

☐ Plus Added Pages for Papers Referred to in Item 4 Above

Number of pages added _____

☐ Plus added pages deleting names of inventor(s) named in prior application(s) who is/are no longer inventor(s) of the subject matter claimed in this application.

Number of pages added _____

☐ Plus "Assignment Cover Letter Accompanying New Application"

Number of pages added _____

☒ **Statement Where No Further Pages Added**

(if no further pages form a part of this Transmittal, then end this Transmittal with this page and check the following item)

☒ This transmittal ends with this page.

METHOD OF CIPHERING DATA TRANSMISSION IN A RADIO SYSTEM

FIELD OF INVENTION

The invention relates to a method of ciphering data transmission in a radio system.

BACKGROUND OF INVENTION

Ciphering is today used in many data transmission systems to prevent the data transmitted from falling into the hands of an unauthorized user. The ciphering has grown in significance in the past few years, particularly as wireless telecommunication has become more common.

The ciphering can be performed, for example, by encrypting the information to be transmitted in a transmitter, and by decrypting the information in a receiver. In the encryption means the information to be transmitted, for example a bit stream, is multiplied by a certain number of encryption bit patterns, whereby it is difficult to find out what the original bit stream was if the encryption bit pattern used is unknown.

In a digital GSM system, for example, ciphering is performed on the radio path: a ciphered bit stream to be transmitted onto the radio path is formed by XORing data bits with ciphering bits, the ciphering bits being formed by an algorithm known per se (the A5 algorithm), using a ciphering key Kc. The A5 algorithm encrypts the information transmitted on the traffic channel and the DCCH control channel.

The ciphering key Kc is set when the network has authenticated the terminal but the traffic on the channel has not yet been ciphered. In the GSM system the terminal is identified on the basis of the International Mobile Subscriber Identity IMSI, which is stored in the terminal, or the Temporary Mobile Subscriber Identity TMSI, which is formed on the basis of the subscriber identity. A subscriber identification key Ki is also stored in the terminal. A terminal identification key is also known to the system.

In order that the ciphering would be reliable, information on the ciphering key Kc must be kept secret. The cipher key is therefore transmitted from the network to the terminal indirectly. A Random Access Number RAND is formed in the network, and the number is then transmitted to the terminal via the base station system. The ciphering key Kc is formed by a known algorithm (the A5 algorithm) from the random access number RAND and the subscriber

identification key Ki. The ciphering key Kc is computed in the same way both in the terminal and in the network part of the system.

In the beginning, data transmission on a connection between the terminal and the base station is thus not ciphered. The ciphering does not start until the base station system sends the terminal a cipher mode command. When the terminal has received the command, it starts to cipher data to be sent and to decipher received data. Correspondingly, the base station system starts to decipher the received data after sending the cipher mode command and to cipher the sent data after the reception and successful decoding of the first ciphered message from the terminal. In the GSM system the cipher mode command comprises a command to start ciphering, and information on the algorithm to be used.

The problem in the known methods is that they have been designed for the present systems, wherefore they are inflexible and not suited for the ciphering of data transmission in new systems, where several parallel services for one mobile station are possible. If we use the same ciphering mask twice for two or more parallel protocol data units that will be sent using the same air interface frame, then an eavesdropper may deduce a lot of information from the data streams. The amount of information that can be deduced depends on the structure of the data streams. From random data that has no structure one cannot obtain any information, but usually there is a structure in the data, especially in the signaling data.

BRIEF DESCRIPTION OF INVENTION

It is an object of the invention to provide a method, and a user equipment and a radio network subsystem implementing the method, solving the above problems. This is achieved with a method of ciphering data transmission in a radio system, comprising: generating a ciphering key; producing a ciphering mask in a ciphering algorithm using the ciphering key as an input parameter; producing ciphered data by applying the ciphering mask to plain data. Using a logical channel specific parameter or a transport channel specific parameter as an additional input parameter to the ciphering algorithm.

The invention also relates to a user equipment, comprising: generating means for generating a ciphering key; a ciphering algorithm connected with the generating means for producing a ciphering mask using the ciphering key as an input parameter; ciphering means connected with the

ciphering algorithm for producing ciphered data by applying the ciphering mask to plain data. The ciphering algorithm uses a logical channel specific parameter or a transport channel specific parameter as an additional input parameter.

The invention further relates to a radio network subsystem, comprising: generating means for generating a ciphering key; a ciphering algorithm connected with the generating means for producing a ciphering mask using the ciphering key as an input parameter; ciphering means connected with the ciphering algorithm for producing ciphered data by applying the ciphering mask to plain data. The ciphering algorithm uses a logical channel specific parameter or a transport channel specific parameter as an additional input parameter.

The preferred embodiments of the invention are claimed in the dependent claims.

Several advantages are achieved with the invention. In the solution of the present invention, ciphering and its properties can be flexibly controlled. The present invention enhances user security in new radio systems. This solution is also better than the known technique, which uses a long enough ciphering mask only once for each air interface frame, because it allows distributed implementation of the needed functionality in the protocol stack.

BRIEF DESCRIPTION OF FIGURES

In the following the invention will be described in greater detail by means of preferred embodiments and with reference to the attached drawings, in which

Figures 1A and 1B illustrate an example of a mobile telephone system;

Figure 2A illustrates a transmitter and a receiver;

Figure 2B illustrates transport channel coding and multiplexing;

Figure 3 illustrates a frame structure;

Figures 4A, 4B and 4C show a block diagram of a ciphering environment according to the invention;

Figure 5 illustrates a mobile station

Figure 6 is a flow diagram illustrating a method according to the invention;

Figure 7A illustrates an example of a protocol stack;

Figure 7B illustrates an example of a protocol stack according to the invention;

Figure 7C illustrates mapping between logical channels and transport channels;

Figure 8 illustrates the structure of a Medium Access Control Layer Protocol Data Unit.

DETAILED DESCRIPTION OF INVENTION

The present invention can be used in different mobile telephone systems. In the following examples, the use of the invention is described in the Universal Mobile Telephone System (UMTS) without restricting the invention to it. The examples illustrate the FDD (Frequency Division Duplex) operation of the UMTS, but do not restrict the invention to it.

With reference to Figures 1A and 1B, a typical mobile telephone system structure will be described. Figure 1B only comprises the blocks that are essential for the description of the invention, although it is apparent to a person skilled in the art that a common mobile telephone system also comprises other functions and structures, which need not be discussed in greater detail here. The main parts of the mobile telephone system are: a core network CN, a UMTS terrestrial radio access network UTRAN, and a user equipment UE. The interface between the CN and the UTRAN is called the Iu interface, and the interface between the UTRAN and the UE is called the Uu interface.

The UTRAN is composed of radio network subsystems RNS. The interface between two RNSs is called the Iur interface. The RNS is composed of a radio network controller RNC and one or more node Bs B. The interface between the RNC and the node B is called the Iub interface. The reception area of the node B, i.e. cell, is denoted in Figure 1A by C.

As the presentation in Figure 1A is very abstract, it is clarified in Figure 1B by setting forth the parts of the GSM system that correspond to the parts of the UMTS. It is clear that the presented mapping is by no means a binding one but an approximation, because the responsibilities and functions of the parts of the UMTS are still being planned.

Figure 1B illustrates a packet switched transmission via Internet 102 from a computer 100 connected with the mobile telephone system to a portable computer 122 connected with a user equipment UE. The user

equipment UE may be a fixedly mounted wireless local loop terminal, a vehicle-mounted terminal or a hand-held portable terminal, for example.

The infrastructure of the radio network UTRAN is composed of radio network subsystems RNS, i.e. base station subsystems. The radio network subsystem RNS is composed of a radio network controller RNC, i.e. a base station controller, and at least one node B, i.e. a base station, under the control of the RNC.

The node B comprises a multiplexer 114, transceivers 116, and a control unit 118 which controls the operation of the transceivers 116 and the multiplexer 114. The multiplexer 114 arranges the traffic and control channels used by a plurality of transceivers 116 on a single transmission connection Iub.

The transceivers 116 of the node B have a connection to an antenna unit 120 which is used for providing a bi-directional (or sometimes one-way) radio connection Uu to a user equipment UE. The structure of the frames transmitted on the radio connection Uu is determined in detail and the connection is referred to as an air interface.

The radio network controller RNC comprises a group switching field 110 and a control unit 112. The group switching field 110 is used for switching speech and data and for connecting signaling circuits. The node B and the radio network controller RNC form a base station subsystem, which additionally comprises a transcoder, also known as a speech codec, or TRAU (Transcoder and Rate Adapter Unit) 108.

The division of the functions and the physical structures of the radio network controller RNC and the node B may differ according to the actual realization of the radio network subsystem. Typically, the node B implements the radio connection. The radio network controller RNC typically manages the following: radio resource control, inter-cell handover control, power control, timing and synchronization, and paging for user equipment.

The transcoder 108 is usually located as close to a mobile switching center 106 as possible because this allows speech to be transmitted between the transcoder 108 and the radio network controller RNC in a cellular radio network form, which saves transmission capacity.

The transcoder 108 converts different digital speech coding modes used between a public switched telephone network and a cellular radio network to make them compatible, for instance from the 64 kbit/s fixed network

form to another form (such as 13 kbit/s) of the cellular radio network, and vice versa. Naturally, the transcoding is carried out only for speech. The control unit 112 carries out call control, mobility management, collection of statistical data and signaling.

The core network CN is composed of the infrastructure belonging to the mobile telephone system which is not part of the UTRAN. Figure 1B illustrates two equipments, which are part of the core network CN, namely a mobile switching center 106, and a gateway mobile switching center 104, which handles mobile telephone system interfaces towards the outside world, in this example towards the Internet 102.

Figure 5 illustrates an exemplary structure of the user equipment UE. The essential parts of the user equipment UE are: an interface 504 to the antenna 502 of the user equipment UE, a transceiver 506, a control part 510 of the user equipment UE, an interface 512 to the battery 514, and a user interface comprising a display 500, a keyboard 508, a microphone 516 and a speaker 518.

Figure 2A illustrates the functioning of a radio transmitter/radio receiver pair. The radio transmitter may be located in the node B or in the user equipment. Correspondingly the radio receiver may be located in the user equipment or in the node B.

The upper portion of Figure 2A illustrates the essential functionality of the radio transmitter. Different services placed in a physical channel are, for example, speech, data, moving or still video picture, and the control channels of the system that are processed in the control part 214 of the radio transmitter. The control part 214 is related to the control of the equipment itself and to the control of the connection. Figure 2A illustrates manipulation of two different transport channels 200A, 200B. Different services call for different source encoding equipment: speech for example calls for a speech codec. For the sake of clarity, source encoding equipment is not, however, presented in Figure 2A.

First the logical channels are ciphered in blocks 216A, 216B. In the ciphering, ciphered data is produced by applying a ciphering mask to plain data. Then the ciphered data is placed in the transport channel in blocks 200A, 200B. As later will be explained with reference to Figures 4A, 4C and 7B the ciphering can be performed either for a logical channel or for a transport channel. Different channels are then channel encoded in blocks 202A and

202B. One form of channel coding is different block codes, one example of which is a cyclic redundancy check, or CRC. Another typical way of performing channel coding is convolutional coding and its different variations, such as punctured convolutional coding and turbo coding.

Having been channel encoded, the channels are interleaved in an interleaver 204A, 204B. The object of the interleaving is to make error correction easier. In the interleaving, the bits are mixed with each other in a predetermined fashion, so that transitory fading on the radio path does not necessarily make the transferred information unidentifiable.

Different signals are multiplexed in block 208 so that they can be sent using the same transmitter.

The interleaved encrypted bits are then spread with a spreading code, scrambled with a scrambling code, and modulated in block 206, whose operation is described in detail in Figure 2B.

Finally, the combined signal is conveyed to the radio frequency parts 210, which may comprise power amplifiers and bandwidth restricting filters. An analog radio signal is then transmitted through an antenna 212 to the radio path Uu.

The lower portion of Figure 2A illustrates the typical functionality of a radio receiver. The radio receiver is typically a Rake receiver. The analog radio signal is received from the radio path Uu by an antenna 234. The received signal is conveyed to radio frequency parts 232, which comprise a filter that blocks the frequencies outside the desired frequency band. A signal is then converted in a demodulator 228 into an intermediate frequency or directly into baseband, and in this form the signal is sampled and quantized.

Because the signal in question is a multipath propagated signal, efforts are made to combine the signal components propagated on different multipaths in block 228, which comprises several Rake fingers.

In a so-called rowing Rake finger, delays for the different multipath propagated signal components are searched. After the delays have been found, different Rake fingers are allocated for receiving each of the multipath propagated signals by correlating the received signal with the used spreading code delayed with the found delay of that particular multipath. The different demodulated and despread multipaths of the same signal are then combined in order to obtain a stronger signal.

The received physical channel is then demultiplexed in a

demultiplexer 224 into data streams of different channels. The channels are then directed each to a de-interleaver 226A, 226B, where the received physical channel is then de-interleaved. After that the physical channels are processed in a specific channel decoder 222A, 222B, where the channel coding used in the transmission is decoded. Convolutional coding is advantageously decoded with a Viterbi decoder. After this the transport channels are mapped to the logical channels in blocks 200A, 200B, or the other possibility is that the deciphering is performed for the transport channels. The channel decoded channels (logical or transport) are deciphered in blocks 220A, 220B by applying a ciphering mask to the received data. Each received logical channel can be further processed, for example, by transferring the data to the computer 122 connected with the user equipment UE. The control channels of the system are conveyed to the control unit 236 of the radio receiver.

Figure 2B illustrates how the transport channels are coded and multiplexed. In principle, Figure 2B is in part the same as Figure 2A but seen from another perspective. In blocks 240A, 240B a Cyclic Redundancy Check is added to each Transport Block. Interleaving is performed in two stages, in blocks 242A, 242B and 246. When two or more services having different quality of service requirements are multiplexed into one or more physical channels, then service specific rate matching 244 is used. In rate matching the channel symbol rates are adjusted to an optimum level, where the minimum quality of service requirement of each service is fulfilled with the same channel symbol energy. Mapping of the transport channels to physical channels is performed in block 248.

As the ciphering is the key issue in the current invention, its principle will be next described in more detail. In Table 1 the first row represents the plain data bits that have to be transmitted to the recipient. The bits on the second row constitute a ciphering mask. The ciphering mask is applied to the plain data, usually by using the exclusive-or operation, i.e. XOR. The resulting ciphered data is on the third row. This ciphered data is sent through the air interface to the recipient. The recipient then performs deciphering by applying the same ciphering mask that has been used in the transmitter to the received data. The fourth row is a ciphering mask that is summed with the third row by using the XOR operation. The resulting recovered data is presented on the fifth row. As we will see, the recovered

data is the same as the plain data.

Plain data	0	1	1	1	0	1	0	0	1	1	1	0	0	1	1	1	0	0	0
Ciphering mask	0	0	1	0	1	0	1	0	0	0	1	0	0	0	0	1	1	1	1
Ciphered data	0	1	0	1	1	1	1	0	1	1	0	0	0	1	1	1	1	1	1
Ciphering mask	0	0	1	0	1	0	1	0	0	0	1	0	0	0	0	1	1	1	1
Recovered data	0	1	1	1	0	1	0	0	1	1	1	0	0	1	1	1	0	0	0

Table 1

Figure 3 shows an example of a frame structure used on a physical channel. Frames 340A, 340B, 340C, 340D are given a running number from one to seventy-two, and they form a 720-millisecond long super frame. The length of one frame 340C is ten milliseconds. The frame 340C is divided into sixteen slots 330A, 330B, 330C, 330D. The length of slot 330C is 0.625 milliseconds. One slot 330C corresponds typically to one power control period, during which the power is adjusted for example by one decibel up or down.

The physical channels are divided into different types, including common physical channels and dedicated physical channels.

The common physical channels are used to carry the following transport channels: PCH, BCH, RACH and FACH.

The dedicated physical channels consist of dedicated physical data channels (DPDCH) 310 and dedicated physical control channels (DPCCH) 312. The DPDCHs 310 are used to carry data 306 generated in layer two of the OSI (Open Systems Interconnection) model and layers above it, i.e. dedicated control channels (DCH). The DPCCHs 312 carry the control information generated in layer one of the OSI model. Control information comprises: pilot bits 300 used in channel estimation, feedback information (FBI) 308 transmit power-control commands (TPC) 302, and optionally a transport format combination indicator (TFCI) 304. The TFCI 304 tells the receiver the transport formats of different transport channels, i.e. Transport Format Combination, used in the current frame.

As can be seen from Figure 3, the down-link DPDCHs 310 and DPCCHs 312 are time multiplexed into the same slot 330C. In the up-link the channels are sent in parallel so that they are IQ/code multiplexed (I = in-phase, Q = quadrature) into each frame 340C.

The channels in the radio interface Uu are processed according to a protocol architecture comprising, according to the ISO (International Standardization Organization) OSI (Open Systems Interconnection) model, three protocol layers: a physical layer (= layer one), a data link layer (= layer two), and a network layer (= layer three). The protocol stacks are located both in the radio network subsystem RNS and in the user equipment UE. Each unit (e.g. user equipment, or radio network subsystem) has a layer which is in logical communication with a layer of another unit. Only the lowest, physical layers communicate with each other directly. The other layers always use the services offered by the next, lower layer. The message must thus physically pass in the vertical direction between the layers, and only in the lowermost layer the message passes horizontally between the layers. Figure 7A illustrates the layers of the protocol architecture. The ovals between different sub-layers indicate service access points (SAP).

The physical layer L1 offers different transport channels to the MAC sub-layer MAC and higher layers. The physical layer transport services are described by how and with what characteristics data is transferred over the radio interface. The transport channels include a Paging Channel PCH, Broadcast Channel BCH, Synchronization Channel SCH, Random Access Channel RACH, Forward Access Channel FACH, Down-link Shared Channel DSCH, Fast Up-link Signaling Channel FAUSCH, and Dedicated Channel DCH. The physical layer L1 maps transport channels with physical channels. In the FDD (Frequency Division Duplex) mode a physical channel is characterized by the code, frequency and, in the up-link, the relative phase (I/Q). In the TDD (Time Division Duplex) mode the physical channel is also characterized by the time slot.

The transport channels may be divided into common channels (where there is a need for in-band identification of the UEs when particular UEs are addressed) and dedicated channels (where the UEs are identified by the physical channel, i.e. code and frequency for the FDD and code, time slot and frequency for the TDD).

The common transport channel types are as follows. The RACH is a contention based up-link channel used for transmission of a relatively small amount of data, for example of initial access or non-real-time dedicated control or traffic data. The FACH is a common down-link channel without closed-loop power control used for transmission of a relatively small amount of

data. The DSCH is a down-link channel shared by several UEs carrying dedicated control or traffic data. The BCH is a down-link channel used for broadcasting system information to an entire cell. The SCH is a down-link channel used for broadcasting synchronization information to an entire cell in the TDD mode. The PCH is a down-link channel used for broadcasting control information to an entire cell allowing efficient UE sleep mode procedures.

The dedicated transport channel types, in turn, are as follows. The DCH is a channel dedicated to one UE used in up-link or down-link. The FAUSCH is an up-link channel used to allocate dedicated channels in conjunction with the FACH. The data link layer is divided into two sub-layers: a MAC sub-layer (Medium Access Control) and a RLC sub-layer (Radio Link Control). The MAC sub-layer L2/MAC offers different logical channels to the RLC sub-layer L2/RLC. The logical channel is characterized by the type of information that is transferred. The logical channels include a Paging Control Channel PCCH, Broadcast Control Channel BCCH, Synchronization Control Channel SCCH, Common Control Channel, Dedicated Control Channel DCCH and Dedicated Traffic Channel DTCH.

The control channels are used for transfer of control plane information only. The SCCH is a down-link channel for broadcasting synchronization information in case of TDD (Time Division Duplex) operation. The BCCH is a down-link channel for broadcasting system control information. The PCCH is a down-link channel that transfers paging information. The CCCH is a bi-directional channel for transmitting control information between the network and the UEs. This channel is commonly used by the UEs having no RRC connection with the network. The DCCH is a point-to-point bi-directional channel that transmits dedicated control information between the UE and the network. This channel is established through an RRC connection setup procedure.

The traffic channels are used for the transfer of user plane information only. The DTCH is a point-to-point channel, dedicated to one UE, for the transfer of user information. A DTCH can exist in both up-link and down-link.

The MAC layer maps logical channels with transport channels. One of the functions of the MAC sub-layer is to select the appropriate transport format for each transport channel depending on the momentary source bit rate.

Figure 7C illustrates mapping between logical channels and transport channels. An SCCH is connected to an SCH. A BCCH is connected to a BCH. A PCCH is connected to a PCH. A CCCH is connected to a RACH and a FACH. A DTCH can be connected to either a RACH and a FACH, to a RACH and a DSCH, to a DCH and a DSCH, or to a DCH. A DCCH can be connected to either a RACH and a FACH, to a RACH and a DSCH, to a DCH and a DSCH, to a DCH, or to a FAUSCH.

The third layer L3 has a RRC sub-layer (Radio Resource Control) that handles the control plane signaling of layer three between the user equipment and the network. Among the functions carried out by the RRC sub-layer are assignment, reconfiguration and release of radio resources for the RRC connection. So the RRC sub-layer handles the assignment of the radio resources required for the RRC connection, including the requirements of both the control and the user plane. The RRC layer may reconfigure radio resources during an established RRC connection.

In the present invention we are interested in the encryption of the different services' data flows of one user. According to the known techniques, all data flows would be encrypted using the same ciphering mask.

The method according to the invention for ciphering data transmission in a radio system is presented in Figure 6. The performance of the method begins in block 600.

In block 602 a ciphering key is generated according to a known technique, for example as described in the Background of the Invention section.

In block 604A a ciphering mask is produced in a ciphering algorithm using the ciphering key as an input parameter. Also a logical channel specific parameter or a transport channel specific parameter is used as an additional input parameter to the ciphering algorithm. The logical channel specific parameter can be one of the following: a Radio Access Bearer Identifier, a Logical Channel Identifier, a Signaling Link Identifier, or some other parameter identifying the logical channel used. The transport channel specific parameter can be, for example, the Dedicated Channel Identifier, or some other parameter identifying the transport channel used.

The term 'bearer' is a high-level name for transmission of information used in connection with a network service. Depending on the services, information in the UMTS can usually be transmitted using one or

more bearers. The services include, for example, speech transmission, data services and video service. A radio bearer, on the other hand, represents that part of the bearer which extends over the air interface. One logical channel normally carries one radio bearer. A logical channel defines the service offered by the MAC layer. A logical channel can be mapped to different types of transport channels depending on the existing service mode (either to a dedicated transport channel or common transport channels). The transport channels define the services offered by the physical layer. It is also possible to multiplex several logical channels into one transport channel in the MAC layer. The transport channels are further mapped to physical channels in the physical layer. Several transport channels can be multiplexed into one physical channel by layer 1. It is also possible that after transport channel multiplexing the data stream is divided between several physical channels.

The invention can thus be applied to a radio system whose terminals can communicate with other transceivers using one or more parallel radio bearers. Typically, when a call is established between a terminal and a network, a physical channel is first established for a Signaling Radio Bearer SRB between the terminal and the radio network subsystem, and once this channel has been established, the actual traffic bearer(s) can be established. The SRB can also be called a signaling link.

The direction of transmission (up-link / down-link) can be used as an additional input parameter to the ciphering algorithm.

Yet another parameter exists: a radio frame specific parameter can be used as an additional input parameter to the ciphering algorithm. The radio frame specific parameter can be, for example, the User Equipment Frame Number (UEFN), or some other parameter identifying the used radio frame. The radio frame specific parameter depends on the protocol layer where the ciphering function is implemented. If it is implemented in the protocol layer that is terminated in the UE and the CN, then a mechanism for conveying the used frame number to the receiving entity has to be defined. If the ciphering function is located in the MAC layer or layer 1 (or some other layer terminated in the UE and the node B or the RNC), a frame number at least partly consisting of the physical frame number can be used, which means that the used frame number need not be signaled with the data.

In block 606 ciphered data is produced by applying the ciphering mask to plain data, using for example the XOR operation as described in Table 1.

Next, an elaborated example illustrating the implementation of the ciphering method in the transmitter and in the receiver is explained in connection with Figures 4A, 4B and 4C. Only the relevant points will be illustrated, but it will be clear for a person skilled in the art how ciphering can be performed in various situations for example with different numbers of PDUs.

Figure 4A describes a block diagram defining the basic ciphering environment defined in this invention. Generating means 408 are used for generating a ciphering key 410 according to a known technique. Connected with the generating means 408 there is a ciphering algorithm 400 for producing ciphering masks 412A, 412B, 412C. The ciphering algorithm uses the generated ciphering key 410 as an input parameter. The ciphering algorithm 400 uses a logical channel specific parameter 402A as an additional input parameter.

In the receiver end, the logical channel specific parameter needed for deciphering can be read from an unciphered MAC header, for example from the C/T-field of the MAC header. The structure of the MAC PDU is illustrated in Figure 8. The MAC PDU consists of an optional MAC header 800 and a MAC Service Data Unit (MAC SDU) 802. Both the MAC header and the MAC SDU are of variable size. The content and the size of the MAC header 800 depend on the type of the logical channel, and in some cases none of the parameters in the MAC header 800 are needed. The size of the MAC-SDU 802 depends on the size of the RLC PDU, which is defined during the set-up procedure. The MAC header 800 comprises a C/T-field 804.This option allows efficient MAC multiplexing of different logical channels (or different instances of the same logical channel type) into one transport channel, both into dedicated transport channels and common transport channels. When this method is used, the MAC header is not ciphered, which allows separating the different MAC PDUs in the receiver end and which in the common channel mode allows reading the RNTI (Radio Network Temporary Identity) field that is needed for routing messages to the correct entity in the UTRAN.

Connected with the ciphering algorithm 400 there are ciphering means 416A, 416B, 416C for producing ciphered data 418A, 418B, 418C by

applying the ciphering mask 412A, 412B, 412C to the plain data 414A, 414B, 414C. As can be seen from Figure 4A, the plain data includes Radio Link Control Layer Protocol Data Units from at least two parallel logical channels, and for each logical channel an individual ciphering mask is produced. So in Figure 4A the ciphering masks 412A, 412B and 412C are all different from each other.

In block 420 the ciphered RLC-PDUs are processed through the MAC layer and mapped into one Transport Block Set, i.e. MAC PDU Set.

Another possible solution is one in which the plain data includes one Radio Link Control Layer Protocol Data Unit 414A from only one logical channel, and for said logical channel an individual ciphering mask 412A is produced. So the invention also works for the individual logical channel.

Normally a new ciphering mask is produced for each radio frame of the physical layer of the protocol stack. If interleaving is used, then a new ciphering mask can be produced for each interleaving period of the physical layer of the protocol stack. Typically one interleaving period consists of several radio frames.

The left-hand side of Figure 4A represents the operations carried out in the transmitter. The corresponding operations will also be carried out in the receiver, as illustrated on the right-hand side of Figure 4A. The only differences are that block 422 is used to derive RLC-PDUs out of the received Transport Block Set, and that the deciphering means 424A, 424B, 424C are used to decipher the received data.

In one embodiment of the invention, a Radio Link Control Layer Protocol Data Unit of at least one logical channel is already ciphered, and the step of producing ciphered data is not repeated for said already ciphered Radio Link Control Layer Protocol Data Unit. It is thus avoided that the data would be ciphered twice. Of course, if for example such end-to-end ciphering is used, the data can be ciphered twice: first by the application using the service, and then by the MAC layer according to the invention. This will cause no loss of transmission capacity, as the XOR operation does not add any extra bits, even if it is performed twice.

Figure 4B illustrates a solution to a situation where the plain data includes at least two successive Radio Link Control Layer Protocol Data Units of one logical channel. If we assume, for example, that the first RLC PDU 414A and the second RLC PDU 414B are from one logical channel, then the

problem can be solved in such a way that only one ciphering mask 412A is produced for these PDUs 414A, 414B. Different parts of this ciphering mask 412A are then used for ciphering the first PDU 414A and the second PDU 414B. The length of the required ciphering mask 412A in this case is naturally the sum of the lengths of the first and the second PDU 414A, 414B. Because the PDUs 414A, 414B are from the same logical channel (same Radio Access Bearer), the maximum length required can be calculated as being two times the maximum RLC PDU size of that bearer.

Figure 4C illustrates a situation where the plain data includes one Transport Block Set (TBS) including Medium Access Control Layer Protocol Data Units of at least two different logical channels, and for each Transport Block Set one ciphering mask 412 is used in producing the ciphered data. In this option, the basic unit to be ciphered is a Transport Block Set. This defines the required length of the ciphering mask 412 produced by the algorithm 400. Layer 1 still adds Transport Block specific CRCs (Cyclic Redundancy Check), but because the XOR operation does not change the length of data, it should be possible to cipher the whole TBS as one unit. The length of each transport block in the TBS has to be told to L1 anyway. This option has the disadvantage that the MAC header is also ciphered, and so the MAC PDUs cannot be routed anywhere on the network side before the TBS is deciphered. This is a problem if common channels over Iur are possible. The length of the required ciphering mask 412 is equal to the maximum Transport Block Set size for the transport channel in question.

Another possible solution is one in which the plain data includes one Transport Block Set including a Medium Access Control Layer Protocol Data Unit of one logical channel, and for each Transport Block Set one ciphering mask is used in producing the ciphered data.

The solution of the invention is implemented in the radio system preferably by software, whereby the invention requires certain functions in the protocol processing software located in the transmitter and in the receiver, especially in blocks 204A, 204B and 226A, 226B of Figure 2A. Thus the generating means 408, the ciphering algorithm 400, and the ciphering means 416A, 416B, 416C can be software modules of the protocol stack residing in the user equipment UE and in the radio network subsystem RNS. The solution can also be implemented with hardware, for example using ASIC (Application Specific Integrated Circuit) or discrete components.

The method of the invention can be implemented, for example, in the Medium Access Control Layer of the protocol stack. This is illustrated in Figure 7B, which shows a high-level overview of the MAC layer depicted in Figure 7A with ciphering functions included. C1() and C2() are two alternatives for the location of ciphering. C1(0), C1(1), C1(2) and C1(3) refer to the use of logical channel specific ciphering parameters as explained above with reference to Figures 4A and 4B, whereas C2(00), C2(01) and C2(02) refer to the use of transport channel specific ciphering parameters. Some MAC functions may be needed below C2(00), C2(01) and C2(02) blocks, but for the sake of clarity they are not illustrated here. Basically the RLC PDUs come to the MAC layer from each logical channel. In the MAC layer the RLC-PDUs are then mapped to the MAC PDUs in the functional blocks 700, 702, 704, which include the operations for the PCH, BCH, SCH, Dedicated Channel and Common Channel operations. Normally one RLC PDU is mapped to one MAC PDU (= Transport Block). This mapping realizes the mapping from a logical channel to a transport channel. The mapping rules have been explained above in connection with Figure 7C. If ciphering is used for the CCCH then a ciphering block, for example C1(4), should be in Figure 7B in the line between the 'CCCH' and the functional block 704.

Even though the invention is described above with reference to an example shown in the attached drawings, it is apparent that the invention is not restricted to it, but can vary in many ways within the inventive idea disclosed in the attached claims.

CLAIMS

1. A method of ciphering data transmission in a radio system, comprising:

(602) generating a ciphering key;

(604A) producing a ciphering mask in a ciphering algorithm using the ciphering key as an input parameter;

(606) producing ciphered data by applying the ciphering mask to plain data;

(604B) using a logical channel specific parameter or a transport channel specific parameter as an additional input parameter to the ciphering algorithm.

2. The method as claimed in claim 1, further comprising:

using the direction of transmission as an additional input parameter to the ciphering algorithm.

3. The method as claimed in claim 1, wherein the logical channel specific parameter is one of the following: a Radio Access Bearer Identifier, a Logical Channel Identifier, a Signaling Link Identifier.

4. The method as claimed in claim 1, wherein the transport channel specific parameter is a Dedicated Channel Identifier.

5. The method as claimed in claim 1, further comprising:

using a radio frame specific parameter as an additional input parameter to the ciphering algorithm.

6. The method as claimed in claim 5, wherein the radio frame specific parameter is a User Equipment Frame Number.

7. The method as claimed in claim 1, wherein the plain data includes Radio Link Control Layer Protocol Data Units from at least two parallel logical channels, and for each logical channel an individual ciphering mask is produced.

8. The method as claimed in claim 7, wherein a Radio Link Control Layer Protocol Data Unit of at least one logical channel is already ciphered, and the step of producing ciphered data is not repeated for said already ciphered Radio Link Control Layer Protocol Data Unit.

9. The method as claimed in claim 1, wherein the plain data includes one Radio Link Control Layer Protocol Data Unit from one logical channel, and for said logical channel an individual ciphering mask is produced.

10. The method as claimed in claim 1, wherein the plain data includes at least two successive Radio Link Control Layer Protocol Data Units of one logical channel, and for each Radio Link Control Layer Protocol Data Unit a different part of the ciphering mask is used in producing the ciphered data.

11. The method as claimed in claim 1, wherein the plain data includes one Transport Block Set including Medium Access Control Layer Protocol Data Units of at least two different logical channels, and for each Transport Block Set one ciphering mask is used in producing the ciphered data.

12. The method as claimed in claim 1, wherein the plain data includes one Transport Block Set including a Medium Access Control Layer Protocol Data Unit of one logical channel, and for each Transport Block Set one ciphering mask is used in producing the ciphered data.

13. The method as claimed in claim 1, wherein the ciphering is performed in the Medium Access Control Layer of a protocol stack.

14. The method as claimed in claim 1, wherein a new ciphering mask is produced for each radio frame of the physical layer of the protocol stack.

15. The method as claimed in claim 1, wherein a new ciphering mask is produced for each interleaving period of the physical layer of the protocol stack.

16. A user equipment (UE), comprising:

generating means (408) for generating a ciphering key (410);

a ciphering algorithm (400) connected with the generating means (408) for producing a ciphering mask (412A, 412B, 412C) using the ciphering key (410) as an input parameter;

ciphering means (416A, 416B, 416C) connected with the ciphering algorithm (400) for producing ciphered data (418A, 418B, 418C) by applying the ciphering mask (412A, 412B, 412C) to plain data (414A, 414B, 414C);

the ciphering algorithm (400) uses a logical channel specific parameter (402A) or a transport channel specific parameter (402B) as an additional input parameter.

17. The user equipment as claimed in claim 16, wherein the ciphering algorithm (400) uses the direction of transmission as an additional input parameter.

18. The user equipment as claimed in claim 16, wherein the logical channel specific parameter (402A) is one of the following: a Radio Access Bearer Identifier, a Logical Channel Identifier, a Signaling Link Identifier.

19. The user equipment as claimed in claim 16, wherein the transport channel specific parameter (402B) is a Dedicated Channel Identifier.

20. The user equipment as claimed in claim 16, wherein the ciphering algorithm (400) uses a radio frame specific parameter (404) as an additional input parameter.

21. The user equipment as claimed in claim 20, wherein the radio frame specific parameter (404) is a User Equipment Frame Number.

22. The user equipment as claimed in claim 16, wherein the ciphering means (416A, 416B, 416C) accept plain data (414A, 414B, 414C) including Radio Link Control Layer Protocol Data Units from at least two parallel logical channels, and the ciphering algorithm (400) produces for each logical channel an individual ciphering mask (412A, 412B, 412C), and the ciphering means (416A, 416B, 416C) use for each logical channel the ciphering mask (412A, 412B, 412C) of said channel.

23. The user equipment as claimed in claim 22, wherein a Radio Link Control Layer Protocol Data Unit (414C) of at least one logical channel is already ciphered, and the ciphering means (416C) do not cipher said already ciphered Radio Link Control Layer Protocol Data Unit (414C).

24. The user equipment as claimed in claim 16, wherein the ciphering means (416A) accept plain data (414A) including a Radio Link Control Layer Protocol Data Unit from one logical channel, and the ciphering algorithm (400) produces for said logical channel an individual ciphering mask (412A), and the ciphering means (416A) use for said logical channel the ciphering mask (412A) of said channel.

25. The user equipment as claimed in claim 16, wherein the ciphering means (426) accept plain data including at least two successive Radio Link Control Layer Protocol Data Units of one logical channel, and the ciphering algorithm (400) produces for said logical channel an individual ciphering mask (412A), and the ciphering means (426) use for each Radio Link Control Layer Protocol Data Unit different part of the ciphering mask (412A).

26. The user equipment as claimed in claim 16, wherein the ciphering means (434) accept plain data including one Transport Block Set

including Medium Access Control Layer Protocol Data Units of at least two different logical channels, and the ciphering algorithm (400) produces for each Transport Block Set an individual ciphering mask (412), and the ciphering means (434) use for each Transport Block Set one ciphering mask (412).

27. The user equipment as claimed in claim 16, wherein the ciphering means (434) accept plain data including one Transport Block Set including a Medium Access Control Layer Protocol Data Unit of one logical channel, and the ciphering algorithm (400) produces for each Transport Block Set an individual ciphering mask (412), and the ciphering means (434) use for each Transport Block Set one ciphering mask (412).

28. The user equipment as claimed in claim 16, wherein the generating means (408), the ciphering algorithm (400), and the ciphering means (416A, 416B, 416C) reside in the Medium Access Control Layer of a protocol stack.

29. The user equipment as claimed in claim 16, wherein the ciphering algorithm (400) produces a new ciphering mask (412A, 412B, 412C) for each radio frame of the physical layer of the protocol stack.

30. The user equipment as claimed in claim 16, wherein the ciphering algorithm (400) produces a new ciphering mask (412A, 412B, 412C) for each interleaving period of the physical layer of the protocol stack.

31. A radio network subsystem (RNS), comprising:

generating means (408) for generating a ciphering key (410);

a ciphering algorithm (400) connected with the generating means (408) for producing a ciphering mask (412A, 412B, 412C) using the ciphering key (410) as an input parameter;

ciphering means (416A, 416B, 416C) connected with the ciphering algorithm (400) for producing ciphered data (418A, 418B, 418C) by applying the ciphering mask (412A, 412B, 412C) to plain data (414A, 414B, 414C);

the ciphering algorithm (400) uses a logical channel specific parameter (402A) or a transport channel specific parameter (402B) as an additional input parameter.

32. The radio network subsystem as claimed in claim 31, wherein the ciphering algorithm (400) uses the direction of transmission as an additional input parameter.

33. The radio network subsystem as claimed in claim 31, wherein the logical channel specific parameter (402A) is one of the following: a Radio

Access Bearer Identifier, a Logical Channel Identifier, a Signaling Link Identifier.

34. The radio network subsystem as claimed in claim 31, wherein the transport channel specific parameter (402B) is a Dedicated Channel Identifier.

35. The radio network subsystem as claimed in claim 31, wherein the ciphering algorithm (400) uses a radio frame specific parameter (404) as an additional input parameter.

36. The radio network subsystem as claimed in claim 35, wherein the radio frame specific parameter (404) is a User Equipment Frame Number.

37. The radio network subsystem as claimed in claim 31, wherein the ciphering means (416A, 416B, 416C) accept plain data (414A, 414B, 414C) including Radio Link Control Layer Protocol Data Units from at least two parallel logical channels, and the ciphering algorithm (400) produces for each logical channel an individual ciphering mask (412A, 412B, 412C), and the ciphering means (416A, 416B, 416C) use for each logical channel the ciphering mask (412A, 412B, 412C) of said channel.

38. The radio network subsystem as claimed in claim 37, wherein a Radio Link Control Layer Protocol Data Unit (414C) of at least one logical channel is already ciphered, and the ciphering means (416C) do not cipher said already ciphered Radio Link Control Layer Protocol Data Unit (414C).

39. The radio network subsystem as claimed in claim 31, wherein the ciphering means (416A) accept plain data (414A) including a Radio Link Control Layer Protocol Data Unit from one logical channel, and the ciphering algorithm (400) produces for said logical channel an individual ciphering mask (412A), and the ciphering means (416A) use for said logical channel theciphering mask (412A) of said channel.

40. The radio network subsystem as claimed in claim 31, wherein the ciphering means (426) accept plain data including at least two successive Radio Link Control Layer Protocol Data Units of one logical channel, and the ciphering algorithm (400) produces for said logical channel an individual ciphering mask (412A), and the ciphering means (426) use for each Radio Link Control Layer Protocol Data Unit a different part of the ciphering mask (412A).

41. The radio network subsystem as claimed in claim 31, wherein the ciphering means (434) accept plain data including one Transport Block Set

including Medium Access Control Layer Protocol Data Units of at least two different logical channels, and the ciphering algorithm (400) produces for each Transport Block Set an individual ciphering mask (412), and the ciphering means (434) use for each Transport Block Set one ciphering mask (412).

42. The radio network subsystem as claimed in claim 31, wherein the ciphering means (434) accept plain data including one Transport Block Set including a Medium Access Control Layer Protocol Data Unit of one logical channel, and the ciphering algorithm (400) produces for each Transport Block Set an individual ciphering mask (412), and the ciphering means (434) use for each Transport Block Set one ciphering mask (412).

43. The radio network subsystem as claimed in claim 31, wherein the generating means (408), the ciphering algorithm (400), and the ciphering means (416A, 416B, 416C) reside in the Medium Access Control Layer of a protocol stack.

44. The radio network subsystem as claimed in claim 31, wherein the ciphering algorithm (400) produces a new ciphering mask (412A, 412B, 412C) for each radio frame of the physical layer of the protocol stack.

45. The radio network subsystem as claimed in claim 31, wherein the ciphering algorithm (400) produces a new ciphering mask (412A, 412B, 412C) for each interleaving period of the physical layer of the protocol stack.

ABSTRACT

The invention relates to a method of ciphering data transmission in a radio system, and to a user equipment using the method, and to a radio network subsystem using the method. The method includes the steps of: (602) generating a ciphering key; (604A) producing a ciphering mask in a ciphering algorithm using the ciphering key as an input parameter; (604B) using a logical channel specific parameter or a transport channel specific parameter as an additional input parameter to the ciphering algorithm; and (606) producing ciphered data by applying the ciphering mask to plain data.

(Figure 6)

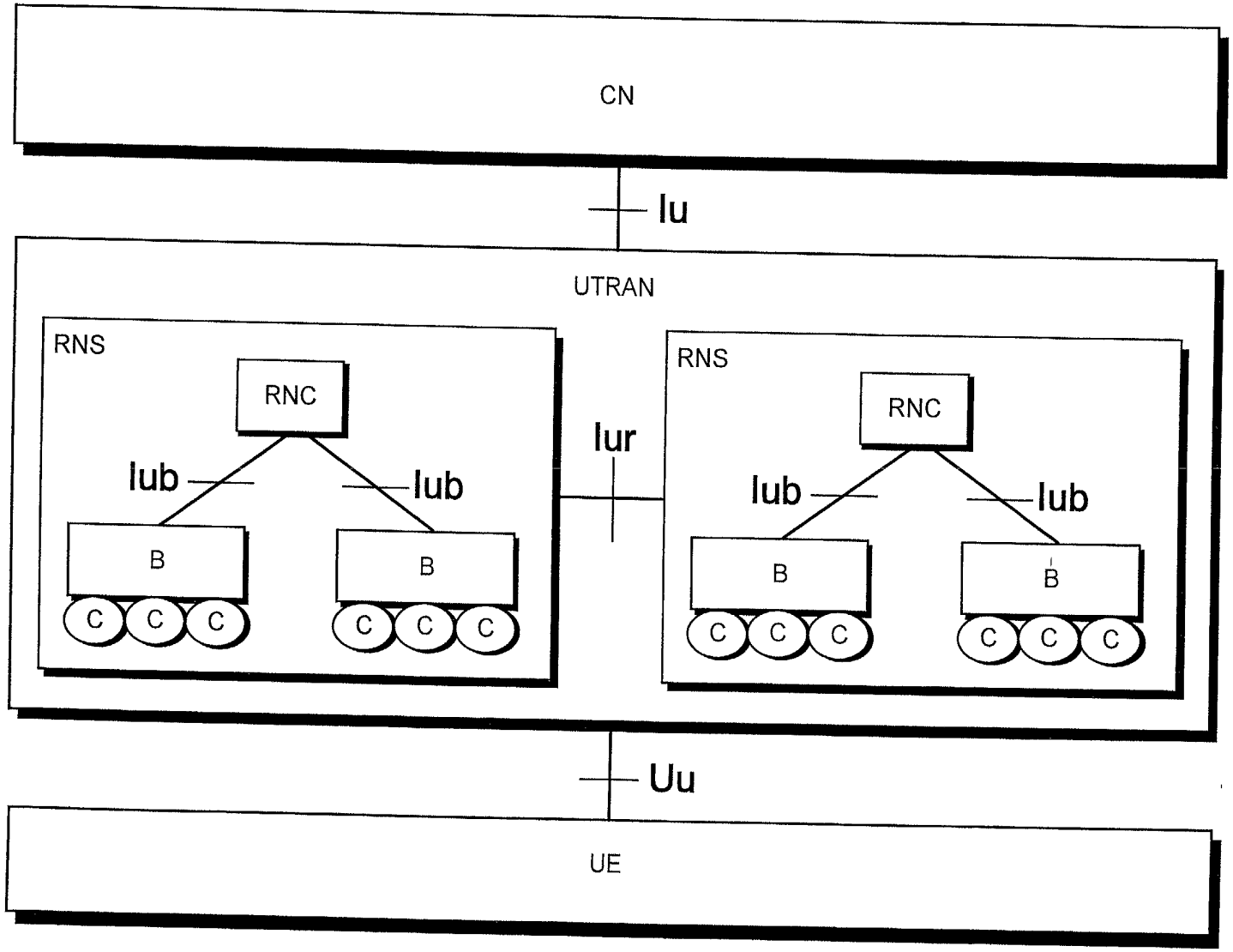
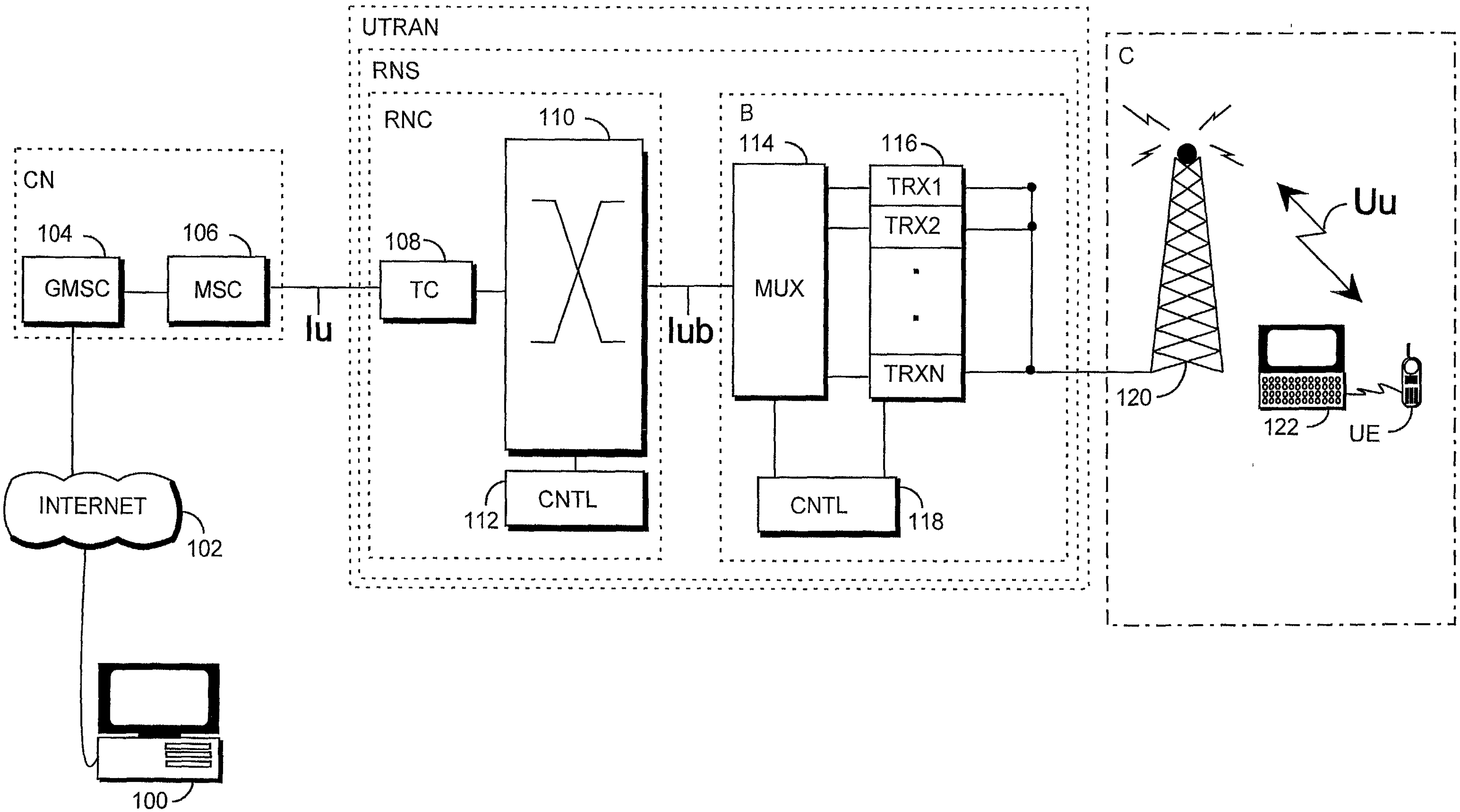


Fig 1A



UTRAN
RNS
RNC
110
108
TC
112
CNTL
B
114
MUX
116
TRX1
TRX2
TRXN
CNTL
118
CN
104
GMSC
106
MSC
Iu
Iub
C
Uu
120
122
UE
INTERNET
102
100

Fig 1B

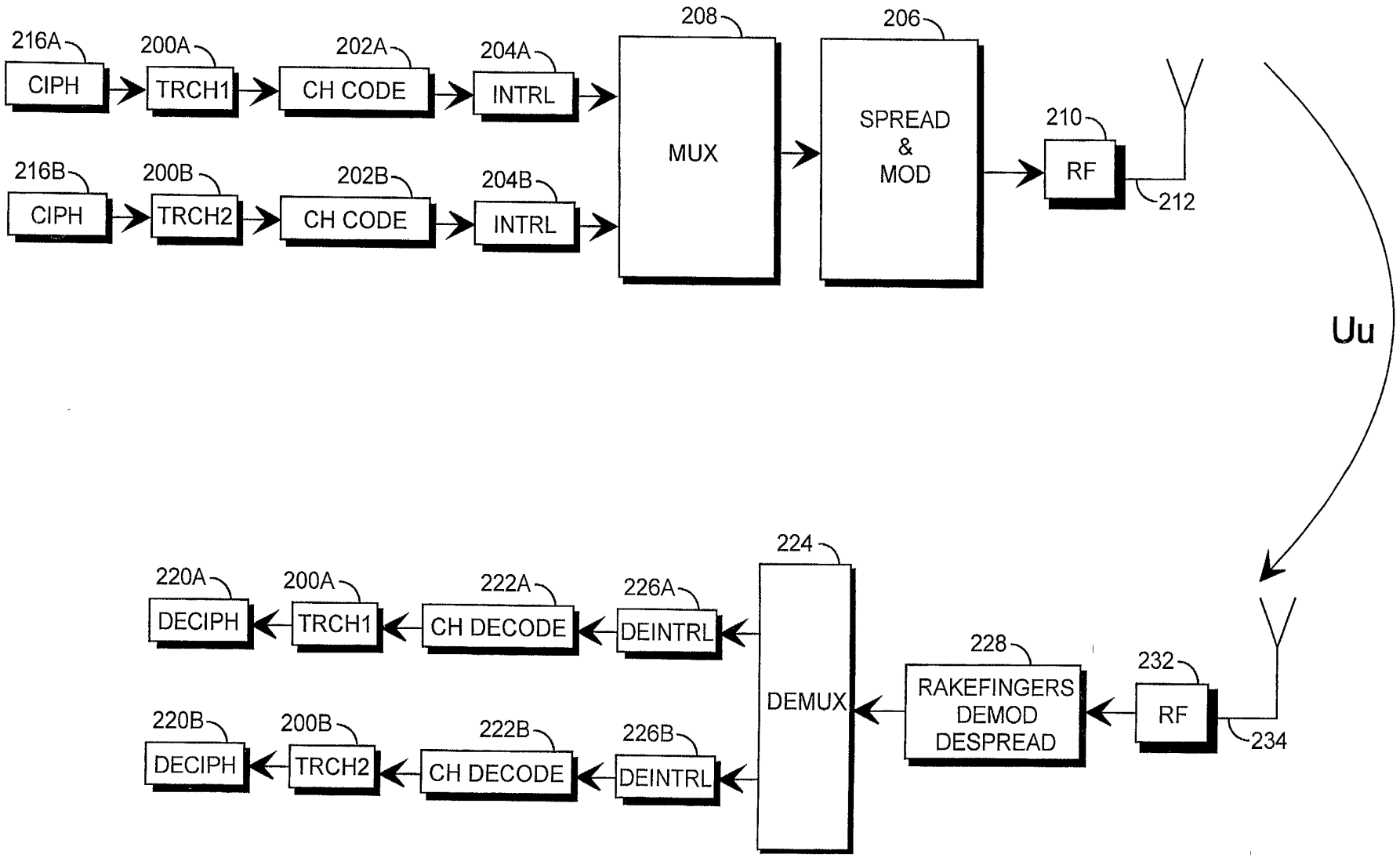

216A
CIPH
200A
TRCH1
202A
CH CODE
204A
INTRL
216B
CIPH
200B
TRCH2
202B
CH CODE
204B
INTRL
208
MUX
206
SPREAD
&
MOD
210
RF
212
Uu
220A
DECIPH
200A
TRCH1
222A
CH DECODE
226A
DEINTRL
224
220B
DECIPH
200B
TRCH2
222B
CH DECODE
226B
DEINTRL
DEMUX
228
RAKEFINGERS
DEMOD
DESPREAD
232
RF
234

Fig 2A

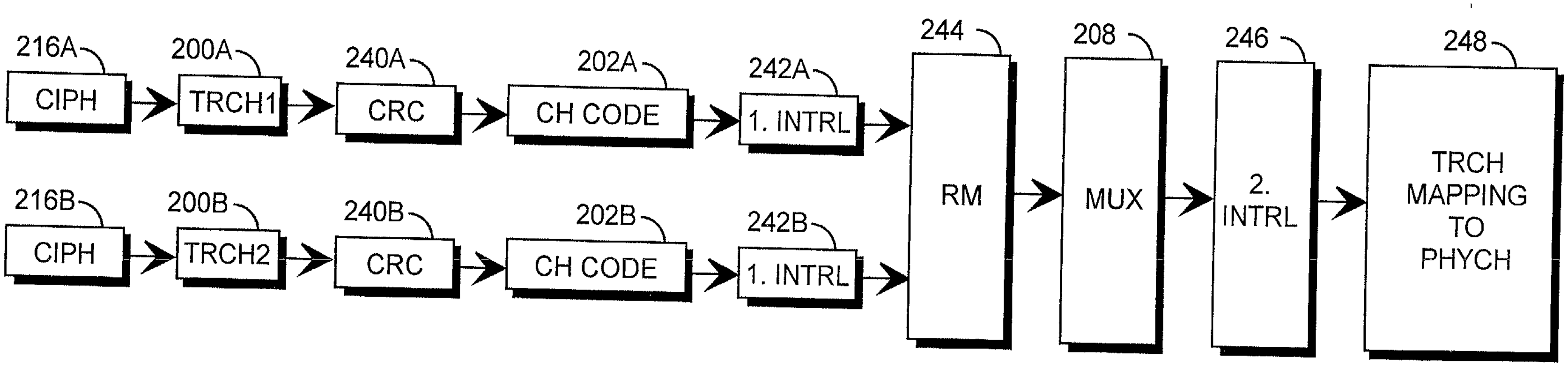

216A
CIPH
200A
TRCH1
240A
CRC
202A
CH CODE
242A
1. INTRL
216B
CIPH
200B
TRCH2
240B
CRC
202B
CH CODE
242B
1. INTRL
244
RM
208
MUX
246
2. INTRL
248
TRCH MAPPING TO PHYCH

Fig 2B

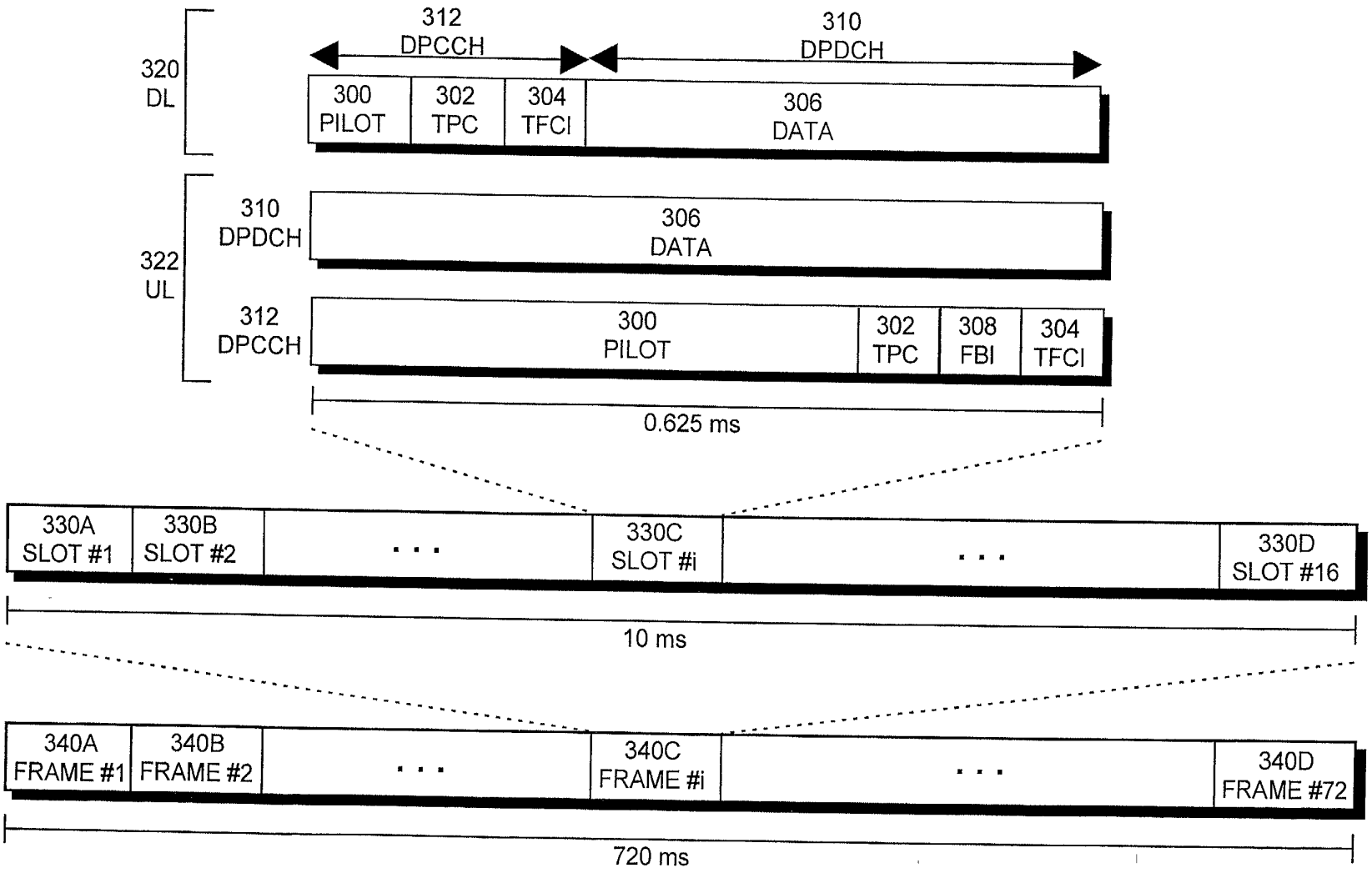

320
DL
312
DPCCH
310
DPDCH
300
PILOT
302
TPC
304
TFCI
306
DATA
322
UL
310
DPDCH
306
DATA
312
DPCCH
300
PILOT
302
TPC
308
FBI
304
TFCI
0.625 ms
330A
SLOT #1
330B
SLOT #2
330C
SLOT #i
330D
SLOT #16
10 ms
340A
FRAME #1
340B
FRAME #2
340C
FRAME #i
340D
FRAME #72
720 ms

Fig 3

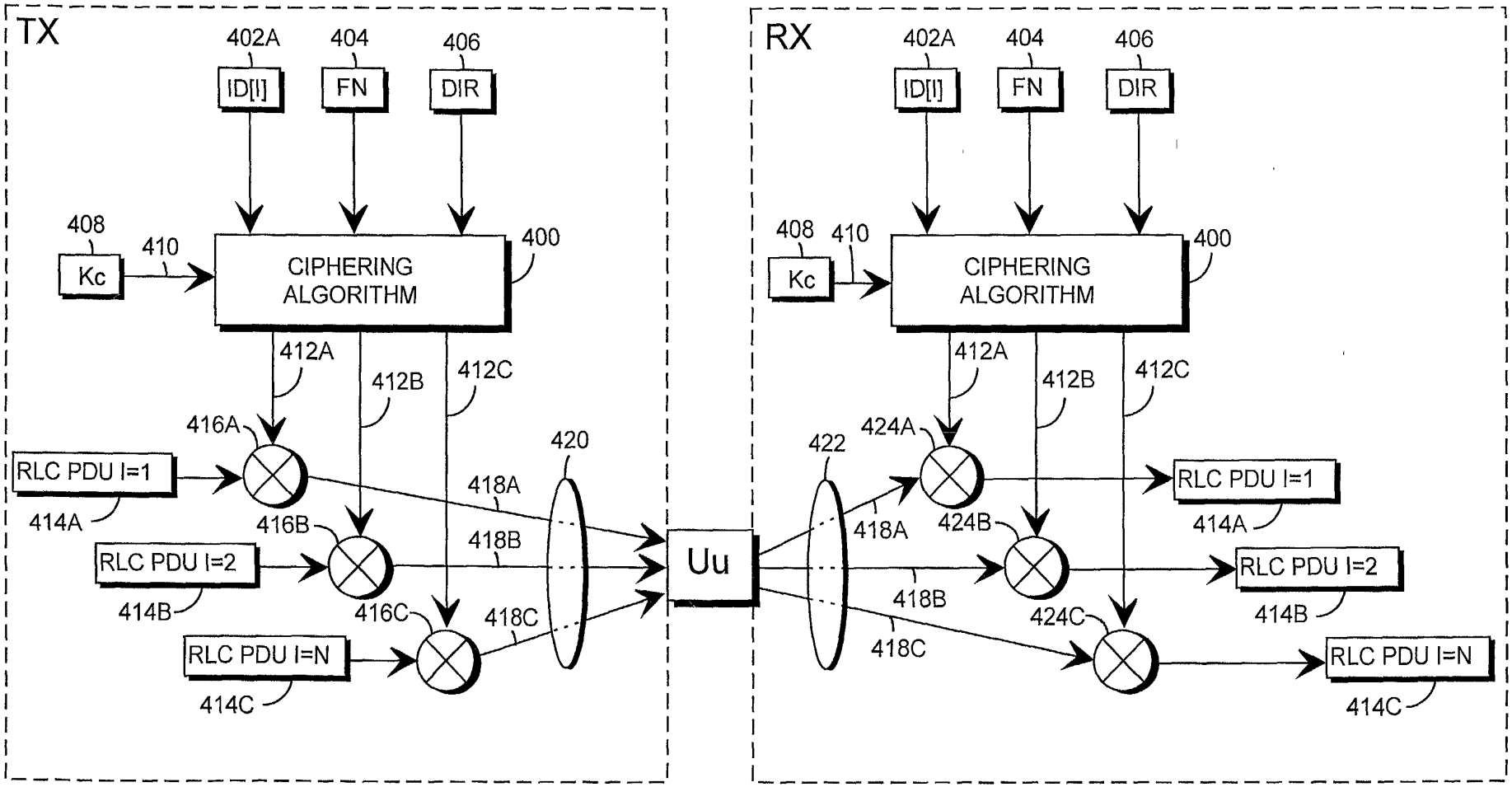

TX
402A
404
406
ID[I]
FN
DIR
408
Kc
410
CIPHERING ALGORITHM
400
412A
412B
412C
416A
416B
416C
420
RLC PDU I=1
414A
418A
RLC PDU I=2
414B
418B
RLC PDU I=N
414C
418C
Uu
RX
402A
404
406
ID[I]
FN
DIR
408
Kc
410
CIPHERING ALGORITHM
400
412A
412B
412C
422
424A
424B
424C
418A
418B
418C
RLC PDU I=1
414A
RLC PDU I=2
414B
RLC PDU I=N
414C

Fig 4A

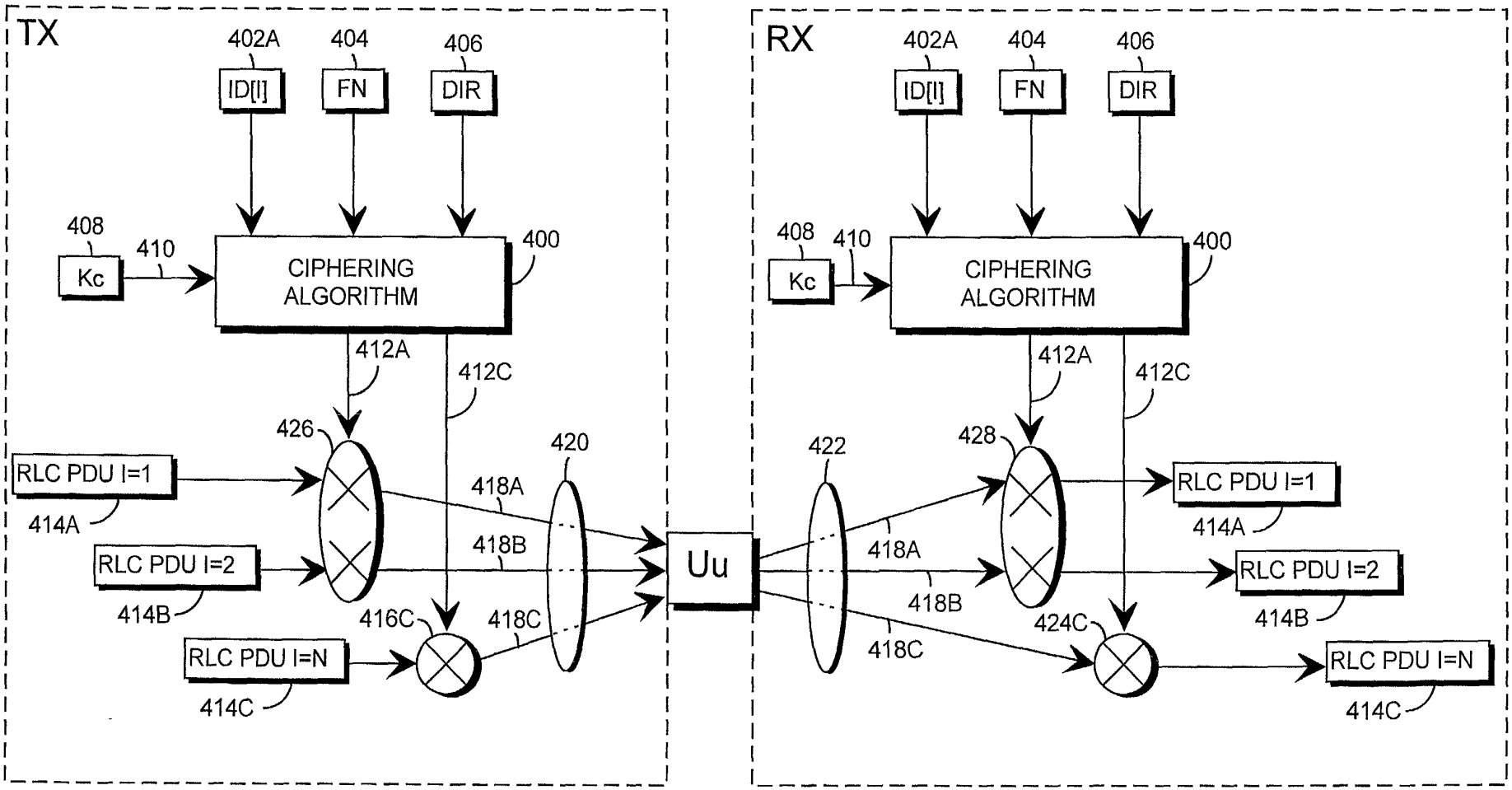

TX
402A
404
406
ID[I]
FN
DIR
408
Kc
410
CIPHERING ALGORITHM
400
412A
412C
426
420
RLC PDU I=1
414A
418A
RLC PDU I=2
414B
418B
416C
418C
RLC PDU I=N
414C
Uu
RX
402A
404
406
ID[I]
FN
DIR
408
Kc
410
CIPHERING ALGORITHM
400
412A
412C
422
428
RLC PDU I=1
414A
418A
RLC PDU I=2
414B
418B
424C
418C
RLC PDU I=N
414C

Fig 4B

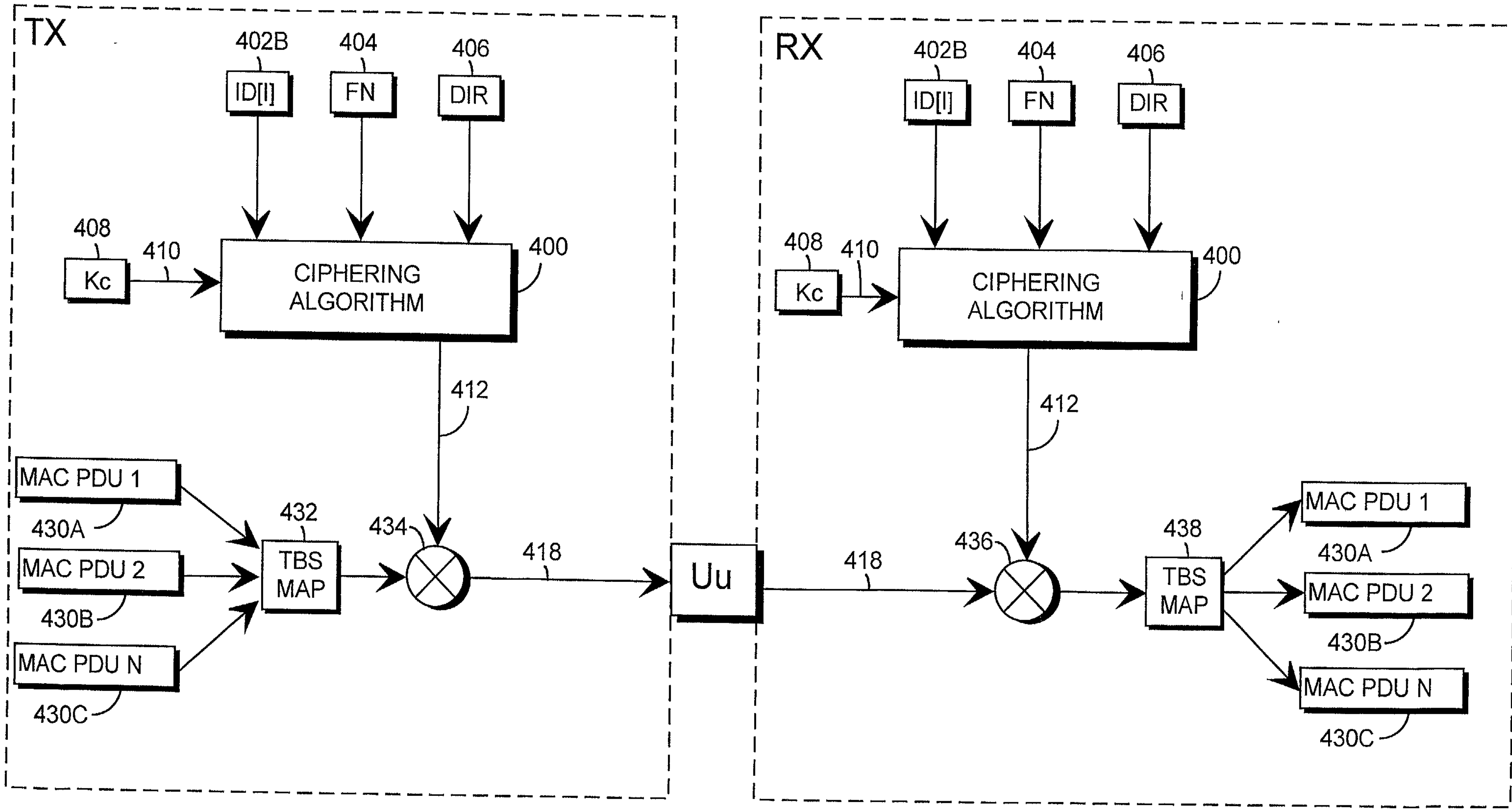

TX
402B
ID[I]
404
FN
406
DIR
408
Kc
410
CIPHERING
ALGORITHM
400
412
MAC PDU 1
430A
MAC PDU 2
430B
MAC PDU N
430C
432
TBS
MAP
434
418
Uu
RX
402B
ID[I]
404
FN
406
DIR
408
Kc
410
CIPHERING
ALGORITHM
400
412
418
436
438
TBS
MAP
MAC PDU 1
430A
MAC PDU 2
430B
MAC PDU N
430C

Fig 4C

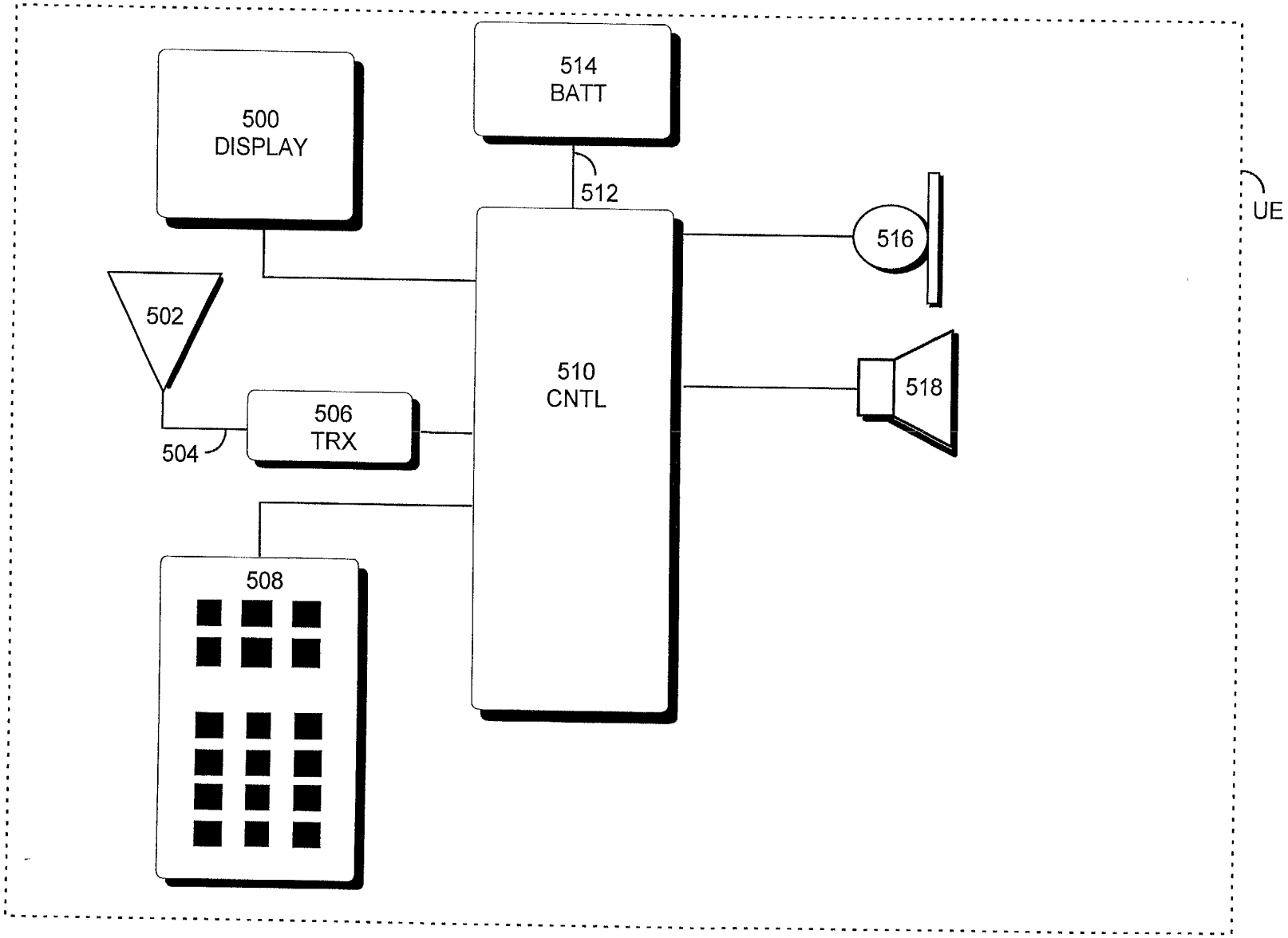


Fig 5

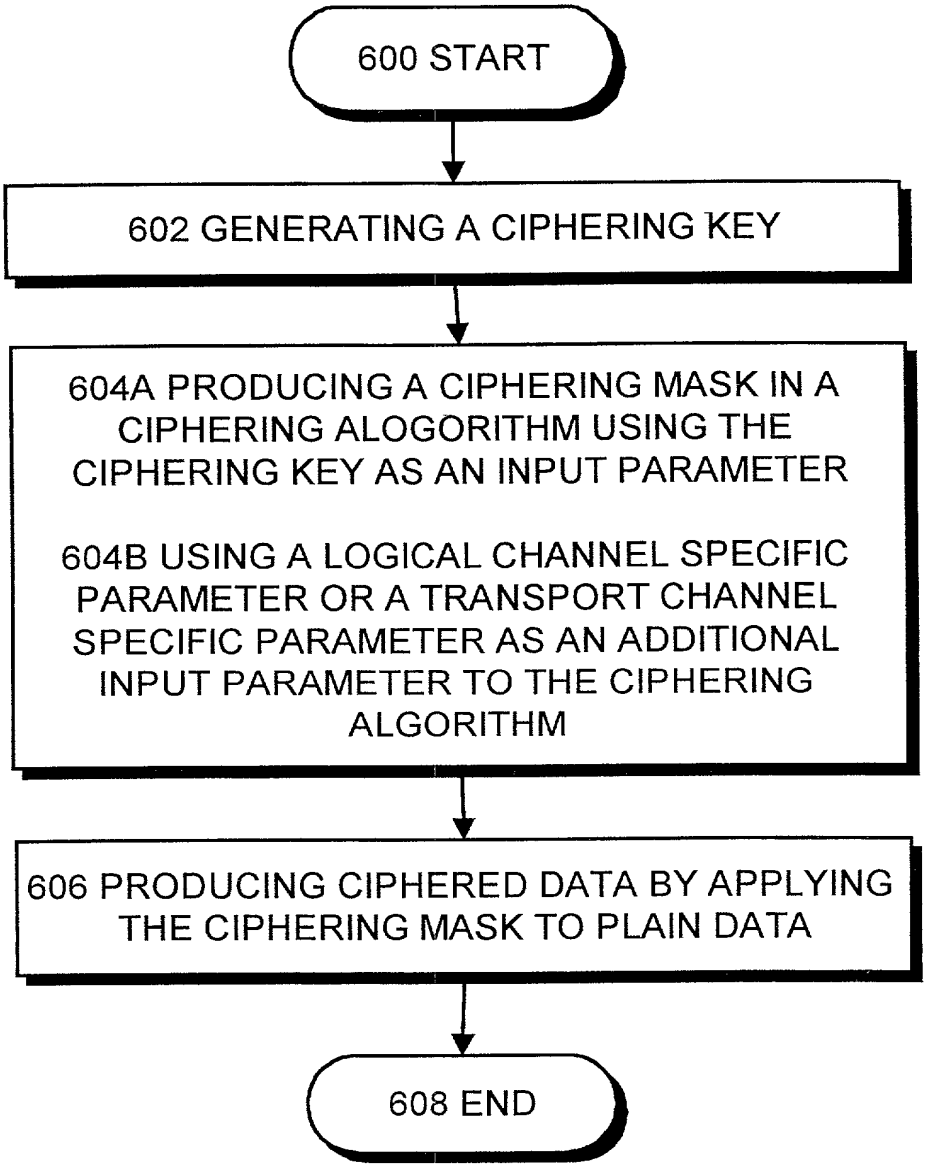

600 START
602 GENERATING A CIPHERING KEY
604A PRODUCING A CIPHERING MASK IN A CIPHERING ALOGORITHM USING THE CIPHERING KEY AS AN INPUT PARAMETER
604B USING A LOGICAL CHANNEL SPECIFIC PARAMETER OR A TRANSPORT CHANNEL SPECIFIC PARAMETER AS AN ADDITIONAL INPUT PARAMETER TO THE CIPHERING ALGORITHM
606 PRODUCING CIPHERED DATA BY APPLYING THE CIPHERING MASK TO PLAIN DATA
608 END

Fig 6

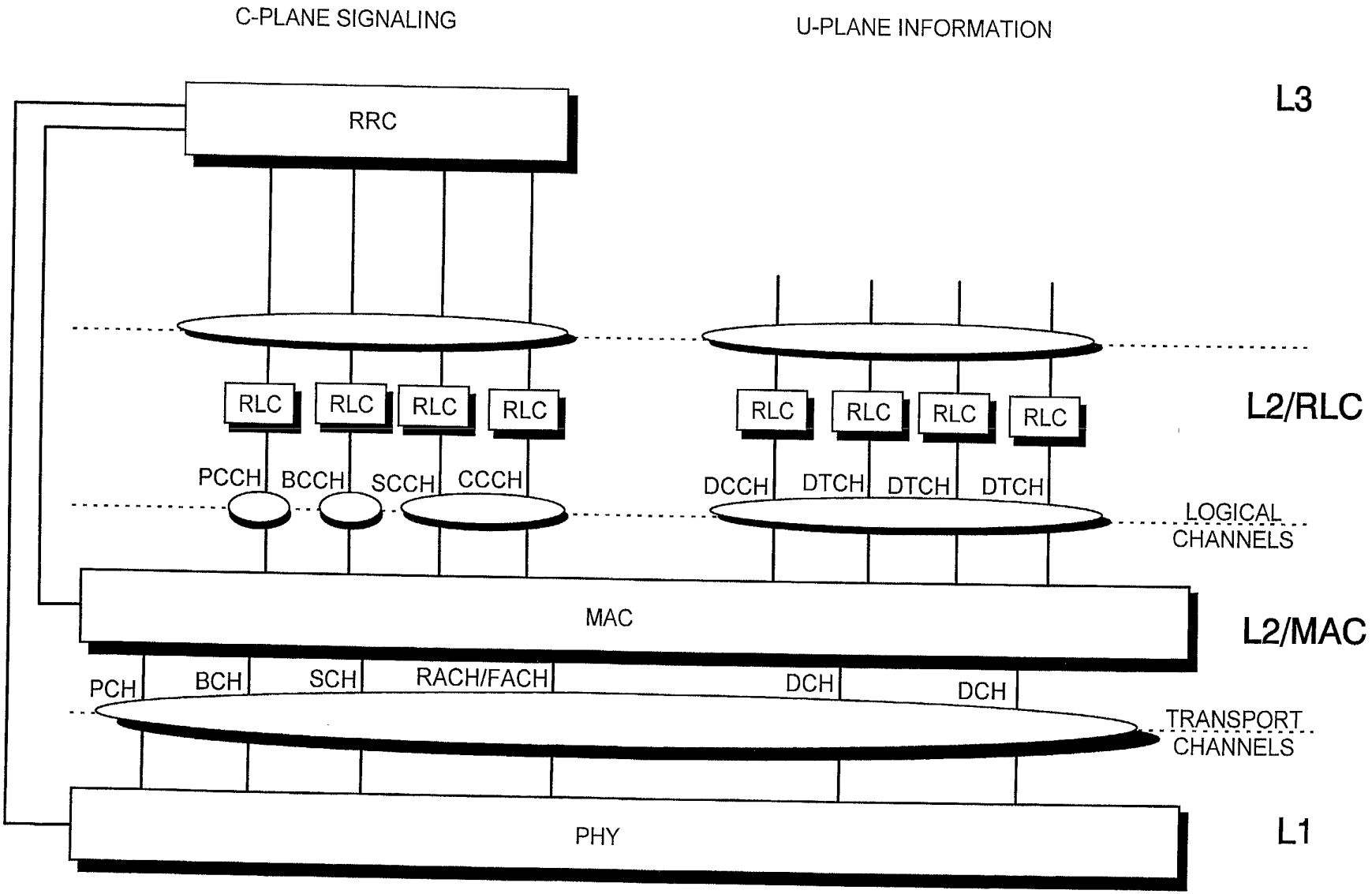


Fig 7A

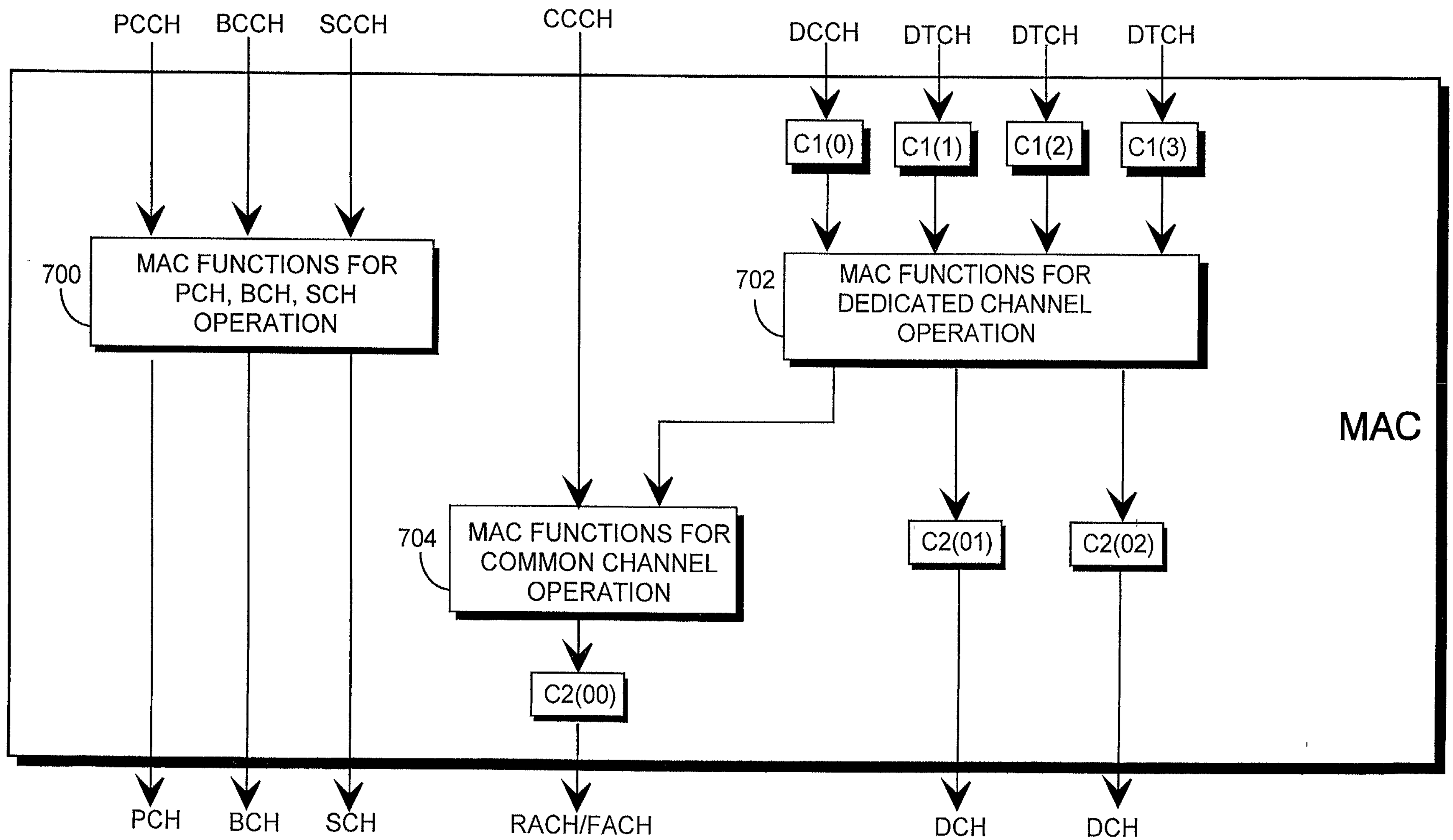


Fig 7B

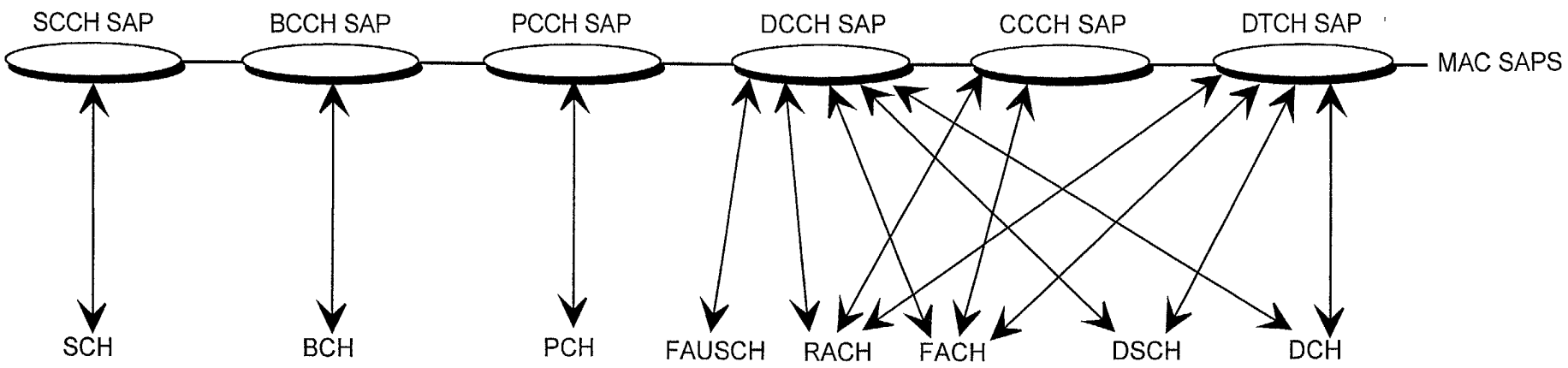


Fig 7C

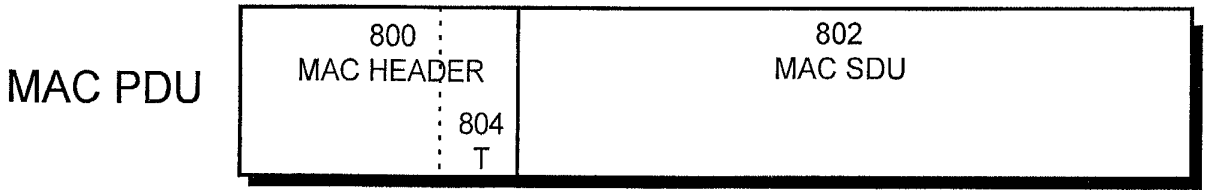


Fig 8

T2990128

Practitioner's Docket No. _____ **PATENT**

COMBINED DECLARATION AND POWER OF ATTORNEY

(ORIGINAL, DESIGN, NATIONAL STAGE OF PCT, SUPPLEMENTAL, DIVISIONAL, CONTINUATION, OR C-I-P)

As a below named inventor, I hereby declare that:

TYPE OF DECLARATION

This declaration is of the following type:

(check one applicable item below)

- [X] original.
- [ ] design.
- [ ] supplemental.

NOTE: If the declaration is for an International Application being filed as a divisional, continuation or continuation-in-part application, do not check next item; check appropriate one of last three items.

- [ ] national stage of PCT.

NOTE: If one of the following 3 items apply, then complete and also attach ADDED PAGES FOR DIVISIONAL, CONTINUATION OR C-I-P.

NOTE: See 37 C.F.R. § 1.63(d) (continued prosecution application) for use of a prior nonprovisional application declaration in the continuation or divisional application being filed on behalf of the same or fewer of the inventors named in the prior application.

- [ ] divisional.
- [ ] continuation.

NOTE: Where an application discloses and claims subject matter not disclosed in the prior application, or a continuation or divisional application names an inventor not named in the prior application, a continuation-in-part application must be filed under 37 C.F.R. § 1.53(b) (application filing requirements — nonprovisional application).

- [ ] continuation-in-part (C-I-P).

INVENTORSHIP IDENTIFICATION

WARNING: *If the inventors are each not the inventors of all the claims, an explanation of the facts, including the ownership of all the claims at the time the last claimed invention was made, should be submitted.*

My residence, post office address and citizenship are as stated below, next to my name. I believe that I am the original, first and sole inventor *(if only one name is listed below)* or an original, first and joint inventor *(if plural names are listed below)* of the subject matter that is claimed, and for which a patent is sought on the invention entitled:

TITLE OF INVENTION

Method of ciphering data transmission in a radio system

SPECIFICATION IDENTIFICATION

the specification of which:

(complete (a), (b), or (c))

(a) ☒ is attached hereto.

NOTE: *"The following combinations of information supplied in an oath or declaration filed on the application filing date with a specification are acceptable as minimums for identifying a specification and compliance with any one of the items below will be accepted as complying with the identification requirement of 37 CFR 1.63:*

"(1) name of inventor(s), and reference to an attached specification which is both attached to the oath or declaration at the time of execution and submitted with the oath or declaration on filing;

"(2) name of inventor(s), and attorney docket number which was on the specification as filed; or

"(3) name of inventor(s), and title which was on the specification as filed."

Notice of July 13, 1995 (1177 O.G. 60).

(b) ☐ was filed on _____, as ☐ Serial No. 0 /_____ or ☐ _____ and was amended on _____ *(if applicable).*

NOTE: *Amendments filed after the original papers are deposited with the PTO that contain new matter are not accorded a filing date by being referred to in the declaration. Accordingly, the amendments involved are those filed with the application papers or, in the case of a supplemental declaration, are those amendments claiming matter not encompassed in the original statement of invention or claims. See 37 CFR 1.67.*

NOTE: *"The following combinations of information supplied in an oath or declaration filed after the filing date are acceptable as minimums for identifying a specification and compliance with any one of the items below will be accepted as complying with the identification requirement of 37 CFR 1.63:*

"(1) name of inventor(s), and application number (consisting of the series code and the serial number, e.g.,08/123,456);

"(2) name of inventor(s), serial number and filing date;

"(3) name of inventor(s) and attorney docket number which was on the specification as filed;

"(4) name of inventor(s), title which was on the specification as filed and filing date;

"(5) name of inventor(s), title which was on the specification as filed and reference to an attached specification which is both attached to the oath or declaration at the time of execution and submitted with the oath or declaration; or

"(6) name of inventor(s), title which was on the specification as filed and accompanied by a cover letter accurately identifying the application for which it was intended by either the application number (consisting of the series code and the serial number, e.g.,08/123,456), or serial number and filing date. Absent any statement(s) to the contrary, it will be presumed that the application filed in the PTO is the application which the inventor(s) executed by signing the oath or declaration."

Notice of July 13, 1995 (1177 O.G. 60).

(c) ☐ was described and claimed in PCT International Application No. _____, filed on _____ and as amended under PCT Article 19 on _____ *(if any).*

SUPPLEMENTAL DECLARATION (37 C.F.R. § 1.67(b))

(complete the following where a supplemental declaration is being submitted)

☐ I hereby declare that the subject matter of the

☐ attached amendment

☐ amendment filed on _____

was part of my/our invention and was invented before the filing date of the original application, above-identified, for such invention.

ACKNOWLEDGEMENT OF REVIEW OF PAPERS AND DUTY OF CANDOR

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information, which is material to patentability as defined in 37, Code of Federal Regulations, § 1.56,

(also check the following items, if desired)

☒ and which is material to the examination of this application, namely, information where there is a substantial likelihood that a reasonable Examiner would consider it important in deciding whether to allow the application to issue as a patent, and

☐ in compliance with this duty, there is attached an information disclosure statement, in accordance with 37 CFR 1.98.

PRIORITY CLAIM (35 U.S.C. §§ 119(a)–(d))

NOTE: "The claim to priority need be in no special form and may be made by the attorney or agent if the foreign application is referred to in the oath or declaration as required by § 1.63. The claim for priority and the certified copy of the foreign application specified in 35 U.S.C. 119(b) must be filed in the case of an interference (§ 1.630), when necessary to overcome the date of a reference relied upon by the examiner, when specifically required by the examiner, and in all other situations, before the patent is granted. If the claim for priority or the certified copy of the foreign application is filed after the date the issue fee is paid, it must be accompanied by a petition requesting entry and by the fee set forth in § 1.17(i). If the certified copy is not in the English language, a translation need not be filed except in the case of interference; or when necessary to overcome the date of a reference relied upon by the examiner, or when specifically required by the examiner, in which event an English language translation must be filed together with a statement that the translation of the certified copy is accurate." 37 C.F.R. § 1.55(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §§ 119(a)–(d) of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed.

(complete (d) or (e))

(d) ☐ no such applications have been filed.

(e) ☒ such applications have been filed as follows.

NOTE: Where item (c) is entered above and the International Application which designated the U.S. itself claimed priority check item (e), enter the details below and make the priority claim.

PRIOR FOREIGN/PCT APPLICATION(S) FILED WITHIN 12 MONTHS (6 MONTHS FOR DESIGN) PRIOR TO THIS APPLICATION AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. § 119(a)-(d)

COUNTRY (OR INDICATE IF PCT)	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 37 USC 119
FI	990500	8 March 1999	☒ YES NO ☐
			☐ YES NO ☐
			☐ YES NO ☐
			☐ YES NO ☐
			☐ YES NO ☐

CLAIM FOR BENEFIT OF PRIOR U.S. PROVISIONAL APPLICATION(S)
(34 U.S.C. § 119(e))

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below:

PROVISIONAL APPLICATION NUMBER — FILING DATE

_____ /_____ _____

_____ /_____ _____

_____ /_____ _____

CLAIM FOR BENEFIT OF EARLIER US/PCT APPLICATION(S) UNDER 35 U.S.C. 120

☐ The claim for the benefit of any such applications are set forth in the attached ADDED PAGES TO COMBINED DECLARATION AND POWER OF ATTORNEY FOR DIVISIONAL, CONTINUATION OR CONTINUATION-IN PART (C-I-P) APPLICATION.

ALL FOREIGN APPLICATION(S), *IF ANY*, FILED MORE THAN 12 MONTHS (6 MONTHS FOR DESIGN) PRIOR TO THIS U.S. APPLICATION

_____

_____

_____

NOTE: If the application filed more than 12 months from the filing date of this application is a PCT filing forming the basis for this application entering the United States as (1) the national stage, or (2) a continuation, divisional, or continuation-in-part, then also complete ADDED PAGES TO COMBINED DECLARATION AND POWER OF ATTORNEY FOR DIVISIONAL, CONTINUATION OR C-I-P APPLICATION for benefit of the prior U.S. or PCT application(s) under 35 U.S.C. § 120.

POWER OF ATTORNEY

I hereby appoint the following practitioner(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

(list name and registration number)

Clarence A. Green (24,622)
Mark F. Harrington (31,686)

(check the following item, if applicable)

☐ I hereby appoint the practitioner(s) associated with the Customer Number provided below to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

☐ Attached, as part of this declaration and power of attorney, is the authorization of the above-named practitioner(s) to accept and follow instructions from my representative(s).

SEND CORRESPONDENCE TO

☒ Address

Clarence A. Green
PERMAN & GREEN, LLP
425 Post Road
Fairfield, CT 06430

☐ Customer Number _____

DIRECT TELEPHONE CALLS TO:
(Name and telephone number)

Clarence A. Green
(203) 259-1800

DECLARATION

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

SIGNATURE(S)

NOTE: Carefully indicate the family (or last) name, as it should appear on the filing receipt and all other documents.

Full name of sole or first inventor

Jukka — (GIVEN NAME) — (MIDDLE INITIAL OR NAME) — Vialen — FAMILY (OR LAST NAME)

Inventor's signature Jukka Vial

Date 7.2.2000 Country of Citizenship Finland

Residence Espoo, Finland

Post Office Address Tyrskykuja 3 B 13, FIN-02320 Espoo, Finland

---

Full name of second joint inventor, if any

Fabio — (GIVEN NAME) — (MIDDLE INITIAL OR NAME) — Longoni — FAMILY (OR LAST NAME)

Inventor's signature Fabio Longoni

Date 7.2.2000 Country of Citizenship Italy

Residence Espoo, Finland

Post Office Address Visamäki 5 E 38, FIN-02130 Espoo, Finland

---

Full name of third joint inventor, if any

(GIVEN NAME) — (MIDDLE INITIAL OR NAME) — FAMILY (OR LAST NAME)

Inventor's signature

Date Country of Citizenship

Residence

Post Office Address

(check proper box(es) for any of the following added page(s) that form a part of this declaration)

☐ **Signature** for fourth and subsequent joint inventors. *Number of pages added* _____.

• • •

☐ **Signature** by administrator(trix), executor(trix) or legal representative for deceased or incapacitated inventor. *Number of pages added* _____.

• • •

☐ **Signature** for inventor who refuses to sign or cannot be reached by person authorized under 37 CFR 1.47. *Number of pages added* _____

• • •

☐ Added page for **signature** by one joint inventor on behalf of deceased inventor(s) where legal representative cannot be appointed in time. (37 CFR 1.47)

• • •

☐ Added pages to combined declaration and power of attorney for divisional, continuation, or continuation-in-part (C-I-P) application.

☐ Number of pages added _____

• • •

☐ Authorization of practitioner(s) to accept and follow instructions from representative.

• • •

(if no further pages form a part of this Declaration, then end this Declaration with this page and check the following item)

☒ This declaration ends with this page.